PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-136231
(43)Date of publication of application : 21.05.1999

(51)Int.Cl. H04L 9/14
G09C 1/00

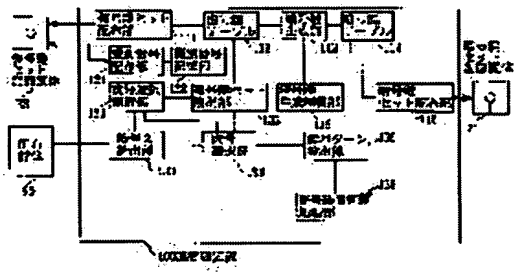
(21)Application number : 10-222656
(22)Date of filing : 06.08.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : TATEBAYASHI MAKOTO

(30)Priority
Priority number : 09211507 Priority date : 06.08.1997 Priority country : JP

(54) ENCRYPTION KEY

(57)Abstract:
PROBLEM TO BE SOLVED: To provide the encryption system where from which kind of an encryption device a distribution medium is produced is identified.
SOLUTION: A decoding selection control section 131 controls an encrypted text read section 133, a decoding key set read section 132, a decoding selection section 134 to repetitively read an encrypted scramble key, to read a decoding key set, and to decode the read scrambled key. As a result, N-sets of keys used to decode N-sets of decoding texts including decoded scramble keys are selected. A key pattern detection section 135 detects one encryption key set coincident with the N-sets of selected key sets among M-sets of encryption key sets stored in an encryption key table 114.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision

of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－136231

(43)公開日　平成11年(1999) 5月21日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ

審査請求　未請求　請求項の数40　ＯＬ　（全 31 頁）

(21)出願番号　特願平10－222656

(22)出願日　平成10年(1998) 8月6日

(31)優先権主張番号　特願平9－211507

(32)優先日　平9 (1997) 8月6日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　舘林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

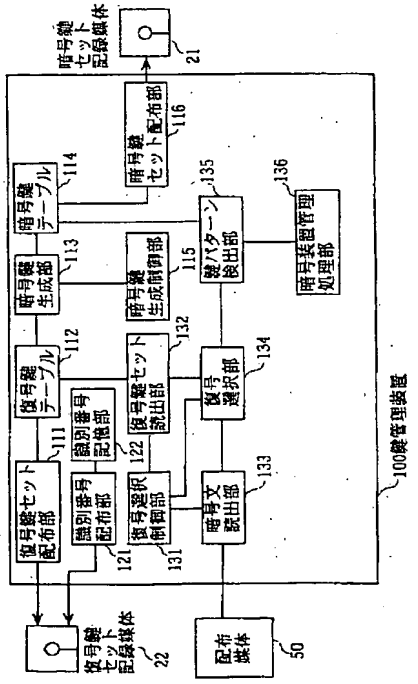
(74)代理人　弁理士　中島　司朗　（外１名）

(54)【発明の名称】　暗号システム

(57)【要約】

【課題】　配布媒体がどの種類の暗号装置により生産されたものであるかを識別することのできる暗号システムを提供することを目的とする。

【解決手段】　復号選択制御部１３１は、暗号文読出部１３３と、復号鍵セット読出部１３２と、復号選択部１３４とに対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返すよう制御する。この結果、Ｎ個の復号されたスクランブルキーを含む復号文が復号される際に用いられたＮ個の鍵のセットが選択される。鍵パターン検出部１３５は、暗号鍵テーブル１１４に記憶されているＭ個の暗号鍵セットから、前記選択されたＮ個の鍵のセットと一致する１つの暗号鍵セットを検出する。



1

【特許請求の範囲】

【請求項１】　１台の鍵管理装置と、Ｍ（Ｍは２以上の整数）種類の暗号装置と、Ｎ（Ｎは２以上の整数）種類の復号装置とからなる暗号システムであって、

前記鍵管理装置は、復号鍵セットをＮ個記憶し、暗号鍵セットをＭ個記憶し、Ｎ個の識別番号を記憶し、前記Ｍ個の暗号鍵セットをそれぞれ前記Ｍ種類の暗号装置に配布し、前記Ｎ個の復号鍵セットをそれぞれ前記Ｎ種類の復号装置に配布し、前記Ｎ個の識別番号をそれぞれ前記Ｎ種類の復号装置に配布し、前記暗号鍵セットはＮ個の暗号鍵からなり、前記復号鍵セットは所定数の復号鍵からなり、

前記Ｍ種類の暗号装置のそれぞれは、デジタルデータをスクランブルキーを用いて暗号化して暗号化デジタルデータを生成し、前記配布された暗号鍵セットを用いて前記スクランブルキーを暗号化してＮ個の暗号化スクランブルキーを生成し、前記暗号化デジタルデータと前記Ｎ個の暗号化スクランブルキーとを配布媒体に書き込み、

前記Ｎ種類の復号装置のそれぞれは、前記配布された復号鍵セットに含まれる前記所定数の復号鍵を用いて、前記配布媒体に含まれ前記配布された識別番号により特定される１つの暗号化スクランブルキーを順次復号し、第１の所定の基準により正しく復号されたスクランブルキーを用いて前記配布媒体に含まれる暗号化デジタルデータを復号してデジタルデータを生成し、識別番号は、配布媒体に書き込まれているＮ個の暗号化スクランブルキーから当該復号装置に対応する１つの暗号化スクランブルキーを識別し、

前記鍵管理装置は、さらに、

前記配布媒体から１つの暗号化スクランブルキーを読み出す第１暗号文読出手段と、

１つの復号鍵セットを読み出す復号鍵セット読出手段と、

前記読み出した復号鍵セットに含まれる前記所定数の復号鍵を用いて、前記読み出した暗号化スクランブルキーを順次復号し、前記第１の所定の基準により正しく暗号化スクランブルキーを復号する復号鍵を、前記所定数の復号鍵の中から１つ選択する復号選択手段と、

前記配布媒体からＮ個の暗号化スクランブルキーの読み出しが終了するまで、前記第１暗号文読出手段、前記復号鍵セット読出手段、前記復号選択手段に対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返し行うように制御し、その結果Ｎ個の復号鍵のセットが選択される第１繰返制御手段と、

前記Ｍ個の暗号鍵セットから、前記選択されたＮ個の復号鍵のセットと一致する１つの暗号鍵セットを検出し、検出された暗号鍵セットにより特定される暗号装置を識別する鍵パターン検出手段とを備えることを特徴とする暗号システム。

2

【請求項２】　前記鍵管理装置は、

所定数の復号鍵からなる復号鍵セットをＮ個記憶している第１復号鍵記憶手段と、

前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、第１の所定の方法により１つの復号鍵を選択して１つの暗号鍵とし、Ｎ個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成手段と、

前記生成された１つの暗号鍵セットを記憶する第１暗号鍵記憶手段と、

Ｍ個の暗号鍵セットが生成されるまで、前記暗号鍵生成手段に対して、暗号鍵セットの生成を繰り返すように制御し、その結果、前記第１暗号鍵記憶手段はＭ個の暗号鍵セットを記憶する第２繰返制御手段と、

前記第１暗号鍵記憶手段に記憶されているＭ個の暗号鍵セットをそれぞれ前記Ｍ種類の暗号装置に配布する暗号鍵セット配布手段と、

前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットをそれぞれ前記Ｎ種類の復号装置に配布する復号鍵セット配布手段と、

Ｎ個の識別番号をそれぞれ前記Ｎ種類の復号装置に配布する識別番号配布手段と備えることを特徴とする請求項１記載の暗号システム。

【請求項３】　前記第１の所定の方法とは、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、ランダムに１個の復号鍵を選択することであることを特徴とする請求項２記載の暗号システム。

【請求項４】　前記第１の所定の方法とは、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、一様にランダムに１個の復号鍵を選択することであることを特徴とする請求項２記載の暗号システム。

【請求項５】　前記Ｍ種類の暗号装置のそれぞれは、

前記鍵管理装置から配布された１つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する第２暗号鍵記憶手段と、

スクランブルキーを生成するスクランブルキー生成手段と、

外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、

前記第２暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるＮ個の暗号鍵を用いて、第２の所定の方法により、前記スクランブルキーを順次暗号化し、Ｎ個の暗号化スクランブルキーを生成する鍵暗号化手段と、

前記生成された暗号化デジタルデータと前記生成されたＮ個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備えることを特徴とする請求項１記載の暗号システム。

【請求項６】　前記第２の所定の方法とは、前記スクラ

ンブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであることを特徴とする請求項５記載の暗号システム。

【請求項７】　前記第２の所定の方法とは、前記スクランブルキーを暗号化してＮ個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化してＮ個の暗号化固定情報を生成することであり、

前記媒体書込手段は、暗号化デジタルデータとＮ個の暗号化スクランブルキーとＮ個の暗号化固定情報とを配布媒体に書き込むことを特徴とする請求項５記載の暗号システム。

【請求項８】　前記復号選択手段は、

前記復号鍵セットから復号鍵を順次読み出す第１復号鍵読出手段と、

前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第１復号文生成手段と、

前記第１の所定の基準により、復号文が正しく復号されているかどうかを検査する第１復号文検査手段と、

前記復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第１復号鍵読出手段、前記第１復号文生成手段、前記第１復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第３繰返制御手段と、

前記復号文検査手段により正しく復号されたと検査された際に用いられた復号鍵を出力する鍵出力手段とを備えることを特徴とする請求項１記載の暗号システム。

【請求項９】　前記第１の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項８記載の暗号システム。

【請求項１０】　前記配布媒体は、さらに、前記暗号鍵セットに含まれるＮ個の暗号鍵を用いて固定値からなる固定情報が暗号化されたＮ個の暗号化固定情報を含み、

前記鍵管理装置は、さらに、

Ｎ個の暗号化固定情報を読み出す暗号化固定情報読出手段と、

前記Ｎ個の復号鍵セットを用いて、前記読み出したＮ個の暗号化固定情報をそれぞれ復号する暗号化固定情報復号手段とを含み、

前記第１の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項８記載の暗号システム。

【請求項１１】　前記Ｎ種類の復号装置のそれぞれは、

前記鍵管理装置から識別番号を受信し、受信した識別番号を記憶する識別番号記憶手段と、

前記鍵管理装置から配布された１つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する第２復号鍵記憶手段と、

前記配布媒体から前記受信した識別番号により識別される１つの暗号化スクランブルキーを読み出す第２暗号文読出手段と、

前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、

前記第２復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す第２復号鍵読出手段と、

前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第２復号文生成手段と、

前記第１の所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文をスクランブルキーとする第２復号文検査手段と、

復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第２復号鍵読出手段、前記第２復号文生成手段、前記第２復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第４繰返制御手段と、

前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えることを特徴とする請求項１記載の暗号システム。

【請求項１２】　前記第１の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項１１記載の暗号システム。

【請求項１３】　前記配布媒体は、さらに、前記暗号鍵セットに含まれるＮ個の暗号鍵を用いて固定値からなる固定情報が暗号化されたＮ個の暗号化固定情報を含み、

前記復号装置は、さらに、

前記識別番号により識別される１つの暗号化固定情報を読み出す暗号化固定情報読出手段と、

前記復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を復号する暗号化固定情報復号手段とを備え、

前記第１の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項１１記載の暗号システム。

【請求項１４】　前記M種類の暗号装置のそれぞれは、

前記鍵管理装置から配布された１つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する第２暗号鍵記憶手段と、

スクランブルキーを生成するスクランブルキー生成手段と、

外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、

前記第２暗号鍵記憶手段に記憶されている暗号鍵セット

に含まれるＮ個の暗号鍵を用いて、第２の所定の方法により、前記スクランブルキーを順次暗号化し、Ｎ個の暗号化スクランブルキーを生成する鍵暗号化手段と、
前記生成された暗号化デジタルデータと前記生成されたＮ個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備え、
前記鍵管理装置において、前記復号選択手段は、
前記復号鍵セットから復号鍵を順次読み出す第１復号鍵読出手段と、
前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第１復号文生成手段と、
前記第１の所定の基準により、復号文が正しく復号されているかどうかを検査する第１復号文検査手段と、
前記復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第１復号鍵読出手段、前記第１復号文生成手段、前記第１復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第３繰返制御手段と、
前記復号文検査手段により正しく復号されたと検査された際に用いられた復号鍵を出力する鍵出力手段とを備えることを特徴とする請求項１記載の暗号システム。
【請求項１５】　前記第１の所定の基準とは、前記復号文に固定情報が含まれることであり、
前記第２の所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであることを特徴とする請求項１４記載の暗号システム。
【請求項１６】　前記第２の所定の方法とは、前記スクランブルキーを暗号化してＮ個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化してＮ個の暗号化固定情報を生成することであり、
前記媒体書込手段は、暗号化デジタルデータとＮ個の暗号化スクランブルキーとＮ個の暗号化固定情報とを配布媒体に書き込み、
前記鍵管理装置は、
Ｎ個の暗号化固定情報を読み出す暗号化固定情報読出手段と、
Ｎ個の復号鍵セットを用いて、前記読み出したＮ個の暗号化固定情報をそれぞれ復号する暗号化固定情報復号手段とを備え、
前記第１の所定の基準とは、Ｎ個の暗号化固定情報を復号し、さらに、固定情報を生成することであることを特徴とする請求項１４記載の暗号システム。
【請求項１７】　前記Ｍ種類の暗号装置のそれぞれは、
前記鍵管理装置から配布された１つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する第２暗号鍵記憶手段と、
スクランブルキーを生成するスクランブルキー生成手段と、

外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、
前記第２暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるＮ個の暗号鍵を用いて、第２の所定の方法により、前記スクランブルキーを順次暗号化し、Ｎ個の暗号化スクランブルキーを生成する鍵暗号化手段と、
前記生成された暗号化デジタルデータと前記生成されたＮ個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備え、
前記Ｎ種類の復号装置のそれぞれは、
前記鍵管理装置から識別番号を受信し、受信した識別番号を記憶する識別番号記憶手段と、
前記鍵管理装置から配布された１つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する第２復号鍵記憶手段と、
前記配布媒体から前記受信した識別番号により識別される１つの暗号化スクランブルキーを読み出す第２暗号文読出手段と、
前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、
前記第２復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す第２復号鍵読出手段と、
前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第２復号文生成手段と、
前記第１の所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文はスクランブルキーを含む第２復号文検査手段と、
復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第２復号鍵読出手段、前記第２復号文生成手段、前記第２復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第４繰返制御手段と、
前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えることを特徴とする請求項１記載の暗号システム。
【請求項１８】　前記第１の所定の基準とは、前記復号文に固定情報が含まれることであり、
前記第２の所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであることを特徴とする請求項１７記載の暗号システム。
【請求項１９】　前記第２の所定の方法とは、前記スクランブルキーを暗号化してＮ個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化

してＮ個の暗号化固定情報を生成することであり、
前記媒体書込手段は、暗号化デジタルデータとＮ個の暗号化スクランブルキーとＮ個の暗号化固定情報とを配布媒体に書き込み、
前記復号装置は、さらに、
前記識別番号により識別される暗号化固定情報を読み出す暗号化固定情報読出手段と、
復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を読み出す暗号化固定情報復号手段とを備え、
前記第１の所定の基準とは、暗号化固定情報を復号し、さらに、固定情報を生成することであることを特徴とする請求項１７記載の暗号システム。

【請求項２０】　前記鍵管理装置は、
所定数の復号鍵からなる復号鍵セットをＮ個記憶している第１復号鍵記憶手段と、
前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、第１の所定の方法により１つの復号鍵を選択して１つの暗号鍵とし、Ｎ個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成手段と、
前記生成された１つの暗号鍵セットを記憶する第１暗号鍵記憶手段と、
Ｍ個の暗号鍵セットが生成されるまで、前記暗号鍵生成手段に対して、暗号鍵セットの生成を繰り返すように制御し、この結果、前記第１暗号鍵記憶手段はＭ個の暗号鍵セットを記憶する第２繰返制御手段と、
前記第１暗号鍵記憶手段に記憶されているＭ個の暗号鍵セットをそれぞれ前記Ｍ種類の暗号装置に配布する暗号鍵セット配布手段と、
前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットをそれぞれ前記Ｎ種類の復号装置に配布する復号鍵セット配布手段と、
識別番号を前記Ｎ種類の復号装置に配布する識別番号配布手段とを備え、
前記Ｎ種類の復号装置のそれぞれは、
前記鍵管理装置から識別番号を受信し、受信した識別番号を記憶する識別番号記憶手段と、
前記鍵管理装置から配布された１つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する第２復号鍵記憶手段と、
前記配布媒体から前記受信した識別番号により識別される１つの暗号化スクランブルキーを読み出す第２暗号文読出手段と、
前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、
前記第２復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す第２復号鍵読出手段と、
前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第２復号文生成手段と、

前記第１の所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文をスクランブルキーとする第２復号文検査手段と、
復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第２復号鍵読出手段、前記第２復号文生成手段、前記第２復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第４繰返制御手段と、
前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えることを特徴とする請求項１記載の暗号システム。

【請求項２１】　前記第１の所定の方法とは、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、ランダムに１個の復号鍵を選択することであることを特徴とする請求項２０記載の暗号システム。

【請求項２２】　前記第１の所定の方法とは、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、一様にランダムに１個の復号鍵を選択することであることを特徴とする請求項２０記載の暗号システム。

【請求項２３】　前記第１の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項２０記載の暗号システム。

【請求項２４】　前記配布媒体は、さらに、前記暗号鍵セットに含まれるＮ個の暗号鍵を用いて固定値からなる固定情報が暗号化されたＮ個の暗号化固定情報を含み、
前記復号装置は、さらに、
前記識別番号により識別される１つの暗号化固定情報を読み出す暗号化固定情報読出手段と、
前記復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を復号する暗号化固定情報復号手段とを備え、
前記第１の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項２０記載の暗号システム。

【請求項２５】　Ｍ（Ｍは２以上の整数）種類の暗号装置とＮ（Ｎは２以上の整数）種類の復号装置に鍵情報を配布する鍵管理装置であって、
所定数の復号鍵からなる復号鍵セットをＮ個記憶している復号鍵記憶手段と、
前記復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、第１の所定の方法により１つの復号鍵を選択して１つの暗号鍵とし、Ｎ個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成手段と、
前記生成された１つの暗号鍵セットを記憶する暗号鍵記

憶手段と、
Ｍ個の暗号鍵セットが生成されるまで、前記暗号鍵生成手段に対して、暗号鍵セットの生成を繰り返すように制御し、その結果、前記暗号鍵記憶手段はＭ個の暗号鍵セットを記憶する繰返制御手段と、
前記第１暗号鍵記憶手段に記憶されているＭ個の暗号鍵セットをそれぞれＭ種類の暗号装置に配布する暗号鍵セット配布手段と、
前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットをそれぞれＮ種類の復号装置に配布する復号鍵セット配布手段と、
Ｎ個の識別番号をそれぞれＮ種類の復号装置に配布する識別番号配布手段とを備えることを特徴とする鍵管理装置。
【請求項２６】　鍵管理装置から配布される鍵情報を用いて、デジタルデータを暗号化して配布媒体に書き込む暗号装置であって、
鍵管理装置から配布された１つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する暗号鍵記憶手段と、
スクランブルキーを生成するスクランブルキー生成手段と、
外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、
前記暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるＮ（Ｎは２以上の整数）個の暗号鍵を用いて、所定の方法により、前記スクランブルキーを順次暗号化し、Ｎ個の暗号化スクランブルキーを生成する鍵暗号化手段と、
前記生成された暗号化デジタルデータと前記生成されたＮ個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備えることを特徴とする暗号装置。
【請求項２７】　鍵管理装置から配布された鍵情報を用いて、配布媒体に書かれた暗号化デジタルデータを復号する復号装置であって、
配布媒体に書き込まれているＮ個の暗号化スクランブルキーから当該復号装置に対応する１つの暗号化スクランブルキーを識別する識別番号を鍵管理装置から受信し、受信した識別番号を記憶する識別番号記憶手段と、
鍵管理装置から配布された１つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する復号鍵記憶手段と、
前記配布媒体から前記受信した識別番号により識別される１つの暗号化スクランブルキーを読み出す暗号文読出手段と、
前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、
前記復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す復号鍵読出手段と、

前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する復号文生成手段と、
所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文はスクランブルキーを含む復号文検査手段と、
復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記復号鍵読出手段、前記復号文生成手段、前記復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する繰返制御手段と、
前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えることを特徴とする復号装置。
【請求項２８】　配布媒体にデジタルデータを暗号化して書き込んだ暗号装置の種類を識別する鍵管理装置であって、
前記配布媒体から１つの暗号化スクランブルキーを読み出す暗号文読出手段と、
１つの復号鍵セットを読み出す復号鍵セット読出手段と、
前記読み出した復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化スクランブルキーを順次復号し、所定の基準により正しく暗号化スクランブルキーを復号する復号鍵を、前記所定数の復号鍵の中から１つ選択する復号選択手段と、
前記配布媒体からＮ個の暗号化スクランブルキーの読み出しが終了するまで、前記暗号文読出手段、前記復号鍵セット読出手段、前記復号選択手段に対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返し行うように制御し、この結果、Ｎ個の復号鍵のセットが選択される繰返制御手段と、
前記Ｍ個の暗号鍵セットから、前記選択されたＮ個の復号鍵のセットと一致する１つの暗号鍵セットを検出し、検出された暗号鍵セットにより特定される暗号装置を識別する鍵パターン検出手段とを備えることを特徴とする鍵管理装置。
【請求項２９】　Ｍ（Ｍは２以上の整数）種類の暗号装置とＮ（Ｎは２以上の整数）種類の復号装置に鍵情報を配布し、所定数の復号鍵からなる復号鍵セットをＮ個記憶している復号鍵記憶手段を備える鍵管理装置において用いられる鍵管理方法であって、
前記復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、所定の方法により１つの復号鍵を選択して１つの暗号鍵とし、Ｎ個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成ステップと、

Ｍ個の暗号鍵セットが生成されるまで、前記暗号鍵生成ステップに対して、暗号鍵セットの生成を繰り返すように制御し、この結果、Ｍ個の暗号鍵セットが生成される繰返制御ステップと、

暗号鍵生成ステップにより生成されたＭ個の暗号鍵セットをそれぞれＭ種類の暗号装置に配布する暗号鍵セット配布ステップと、

前記復号鍵記憶手段に記憶されているＮ個の復号鍵セットをそれぞれＮ種類の復号装置に配布する復号鍵セット配布ステップと、

Ｎ個の識別番号をそれぞれＮ種類の復号装置に配布する識別番号配布ステップとを含むことを特徴とする鍵管理方法。

【請求項３０】　前記所定の方法とは、前記復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、ランダムに１個の復号鍵を選択することであることを特徴とする請求項２９記載の鍵管理方法。

【請求項３１】　前記所定の方法とは、前記復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、一様にランダムに１個の復号鍵を選択することであることを特徴とする請求項２９記載の鍵管理方法。

【請求項３２】　鍵管理装置から配布される鍵情報を用いて、デジタルデータを暗号化して配布媒体に書き込み、鍵管理装置から配布された１つの暗号鍵セットを受信し受信した前記暗号鍵セットを記憶する暗号鍵記憶手段を備える暗号装置において用いられる暗号方法であって、

スクランブルキーを生成するスクランブルキー生成ステップと、

外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化ステップと、

前記暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるＮ（Ｎは２以上の整数）個の暗号鍵を用いて、所定の方法により、前記スクランブルキーを順次暗号化し、Ｎ個の暗号化スクランブルキーを生成する鍵暗号化ステップと、

前記生成された暗号化デジタルデータと前記生成されたＮ個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込ステップとを含むことを特徴とする暗号方法。

【請求項３３】　前記所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであるを含むことを特徴とする請求項３２記載の暗号方法。

【請求項３４】　前記所定の方法とは、前記スクランブルキーを暗号化してＮ個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化してＮ個の暗号化固定情報を生成することであり、

前記媒体書込ステップは、暗号化デジタルデータとＮ個の暗号化スクランブルキーとＮ個の暗号化固定情報とを配布媒体に書き込むことを特徴とする請求項３２記載の暗号方法。

【請求項３５】　鍵管理装置から配布された鍵情報を用いて、配布媒体に書かれた暗号化デジタルデータを復号し、鍵管理装置から識別番号を受信し受信した識別番号を記憶する識別番号記憶手段と、鍵管理装置から配布された１つの復号鍵セットを受信し受信した前記復号鍵セットを記憶する復号鍵記憶手段とを備える復号装置において用いられる復号方法であって、

前記識別番号は配布媒体に書き込まれているＮ個の暗号化スクランブルキーから当該復号装置に対応する１つの暗号化スクランブルキーを識別し、

前記配布媒体から前記受信した識別番号により識別される１つの暗号化スクランブルキーを読み出す暗号文読出ステップと、

前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出ステップと、

前記復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す復号鍵読出ステップと、

前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する復号文生成ステップと、

所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文はスクランブルキーを含む復号文検査ステップと、

復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記復号鍵読出ステップ、前記復号文生成ステップ、前記復号文検査ステップに対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する繰返制御ステップと、

前記復号文検査ステップにより正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号ステップとを含むことを特徴とする復号方法。

【請求項３６】　前記所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項３５記載の復号方法。

【請求項３７】　前記配布媒体は、さらに、暗号鍵セットに含まれるＮ個の暗号鍵を用いて固定値からなる固定情報が暗号化されたＮ個の暗号化固定情報を含み、

前記復号方法は、さらに、

前記識別番号により識別される１つの暗号化固定情報を読み出す暗号化固定情報読出ステップと、

復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を復号する暗号化固定情報復号ステップとを含み、

前記所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報

が含まれることであることを特徴とする請求項３５記載の復号方法。

【請求項３８】　配布媒体にデジタルデータを暗号化して書き込んだ暗号装置の種類を識別する鍵管理装置において用いられる鍵管理方法であって、

前記配布媒体から１つの暗号化スクランブルキーを読み出す暗号文読出ステップと、

１つの復号鍵セットを読み出す復号鍵セット読出ステップと、

前記読み出した復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化スクランブルキーを順次復号し、所定の基準により正しく暗号化スクランブルキーを復号する復号鍵を、前記所定数の復号鍵の中から１つ選択する復号選択ステップと、

前記配布媒体からＮ（Ｎは２以上の整数）個の暗号化スクランブルキーの読み出しが終了するまで、前記暗号文読出ステップ、前記復号鍵セット読出ステップ、前記復号選択ステップに対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返し行うように制御し、この結果、Ｎ個の復号鍵のセットが選択される繰返制御ステップと、

前記Ｍ個の暗号鍵セットから、前記選択されたＮ個の復号鍵のセットと一致する１つの暗号鍵セットを検出し、検出された暗号鍵セットにより特定される暗号装置の種類を識別する鍵パターン検出ステップとを含むことを特徴とする鍵管理方法。

【請求項３９】　前記所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項３８記載の鍵管理方法。

【請求項４０】　前記配布媒体は、さらに、暗号鍵セットに含まれるＮ個の暗号鍵を用いて固定値からなる固定情報が暗号化されたＮ個の暗号化固定情報を含み、

前記鍵管理方法は、さらに、

Ｎ個の暗号化固定情報を読み出す暗号化固定情報読出ステップと、

Ｎ個の復号鍵セットを用いて、前記読み出したＮ個の暗号化固定情報を復号する暗号化固定情報復号ステップとを含み、

前記所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項３８記載の鍵管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタル化された文書、音声、画像、プログラムなどのデジタル著作物を暗号化して伝送媒体や記録媒体を介して伝送する暗号システムに関し、特に、１台の鍵管理装置が、複数の種類の暗号装置と複数の種類の復号装置とを管理する技術に関する。

【０００２】

【従来の技術】従来、デジタル化された文書、音声、画像、プログラムなどのデジタル著作物を市場などに流通させる場合には、デジタル著作物が不正に使用されないように、暗号装置により秘密鍵を用いて暗号化されたデジタル著作物を伝送媒体や記録媒体（以下、配布媒体と呼ぶ。）を介して配布し、復号装置により復号鍵を用いて復号している。

【０００３】

【発明が解決しようとする課題】しかしながら、復号鍵が不正に解読されデジタル著作物が不正に使用されたり、配布媒体が不正に複製される場合がある。このため、暗号システムは、復号鍵が不正に解読されにくくしなければならないという第１の問題点がある。この第１の問題点を解決するためには、異なる暗号鍵を有する暗号装置が複数あるほうがよい。また、暗号装置の保有する鍵の総量は、鍵管理装置の保有する鍵の総量よりも少ないことが望ましい。

【０００４】また、１つの復号装置の復号鍵が解読された場合に、他の復号装置にもその影響が及び、解読された復号鍵が利用されて、他の復号装置において不正にデジタル著作物が利用されるという第２の問題点がある。この第２の問題点を解決するためには、異なる復号装置には、異なる復号鍵が割り当てられることが望ましい。このとき、暗号化されたデータがどのような復号装置においても首尾よく復号できるようにするため、暗号装置が全ての異なる復号装置に対応する暗号鍵を備え、データをそれぞれの暗号鍵で暗号化して複数の暗号化データを生成して配布し、復号装置は、配布される複数の暗号化データから、当該復号装置向けの暗号化データを判別して取り出し、これを復号する暗号システムが提案されている。また、復号装置に、複数の鍵を割り当てる暗号システムが提案されている。さらに、配布媒体が不正に複製された疑いがある場合などに、複製に用いられたオリジナルの配布媒体の生産元や流通経路を特定するために、当該オリジナルの配布媒体の生産に用いられた暗号装置を特定する必要があるという第３の問題点がある。

【０００５】本発明は、上記に示す第１、第２の問題点を解決するため、異なる暗号鍵を有する暗号装置を複数有し、暗号装置の保有する鍵の総量は、鍵管理装置の保有する鍵の総量よりも少なく、異なる復号装置には異なる復号鍵が複数個割り当てられ、さらに、上記に示す第３の問題点を解決するため、配布媒体が不正に複製された疑いがある場合などに、配布媒体がどの種類の暗号装置により生産されたものであるかを識別することのできる暗号システムを提供することを目的とする。

【０００６】

【課題を解決するための手段】上記目的を達成するために、本発明は、１台の鍵管理装置と、Ｍ（Ｍは２以上の

整数）種類の暗号装置と、Ｎ（Ｎは２以上の整数）種類の復号装置とからなる暗号システムであって、前記鍵管理装置は、復号鍵セットをＮ個記憶し、暗号鍵セットをＭ個記憶し、Ｎ個の識別番号を記憶し、前記Ｍ個の暗号鍵セットをそれぞれ前記Ｍ種類の暗号装置に配布し、前記Ｎ個の復号鍵セットをそれぞれ前記Ｎ種類の復号装置に配布し、前記Ｎ個の識別番号をそれぞれ前記Ｎ種類の復号装置に配布し、前記暗号鍵セットはＮ個の暗号鍵からなり、前記復号鍵セットは所定数の復号鍵からなり、前記Ｍ種類の暗号装置のそれぞれは、デジタルデータをスクランブルキーを用いて暗号化して暗号化デジタルデータを生成し、前記配布された暗号鍵セットを用いて前記スクランブルキーを暗号化してＮ個の暗号化スクランブルキーを生成し、前記暗号化デジタルデータと前記Ｎ個の暗号化スクランブルキーとを配布媒体に書き込み、前記Ｎ種類の復号装置のそれぞれは、前記配布された復号鍵セットに含まれる前記所定数の復号鍵を用いて、前記配布媒体に含まれ前記配布された識別番号により特定される１つの暗号化スクランブルキーを順次復号し、第１の所定の基準により正しく復号されたスクランブルキーを用いて前記配布媒体に含まれる暗号化デジタルデータを復号してデジタルデータを生成し、識別番号は、配布媒体に書き込まれているＮ個の暗号化スクランブルキーから当該復号装置に対応する１つの暗号化スクランブルキーを識別し、前記鍵管理装置は、さらに、前記配布媒体から１つの暗号化スクランブルキーを読み出す第１暗号文読出手段と、１つの復号鍵セットを読み出す復号鍵セット読出手段と、前記読み出した復号鍵セットに含まれる前記所定数の復号鍵を用いて、前記読み出した暗号化スクランブルキーを順次復号し、前記第１の所定の基準により正しく暗号化スクランブルキーを復号する復号鍵を、前記所定数の復号鍵の中から１つ選択する復号選択手段と、前記配布媒体からＮ個の暗号化スクランブルキーの読み出しが終了するまで、前記第１暗号文読出手段、前記復号鍵セット読出手段、前記復号選択手段に対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返し行うように制御し、その結果Ｎ個の復号鍵のセットが選択される第１繰返制御手段と、前記Ｍ個の暗号鍵セットから、前記選択されたＮ個の復号鍵のセットと一致する１つの暗号鍵セットを検出し、検出された暗号鍵セットにより特定される暗号装置を識別する鍵パターン検出手段とを備えることを特徴とする。

【０００７】ここで、前記鍵管理装置は、所定数の復号鍵からなる復号鍵セットをＮ個記憶している第１復号鍵記憶手段と、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、第１の所定の方法により１つの復号鍵を選択して１つの暗号鍵とし、Ｎ個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成手段と、前記生成された１つの暗号鍵セットを記憶する第

１暗号鍵記憶手段と、Ｍ個の暗号鍵セットが生成されるまで、前記暗号鍵生成手段に対して、暗号鍵セットの生成を繰り返すように制御し、その結果、前記第１暗号鍵記憶手段はＭ個の暗号鍵セットを記憶する第２繰返制御手段と、前記第１暗号鍵記憶手段に記憶されているＭ個の暗号鍵セットをそれぞれ前記Ｍ種類の暗号装置に配布する暗号鍵セット配布手段と、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットをそれぞれ前記Ｎ種類の復号装置に配布する復号鍵セット配布手段と、Ｎ個の識別番号をそれぞれ前記Ｎ種類の復号装置に配布する識別番号配布手段と備えるように構成してもよい。

【０００８】ここで、前記第１の所定の方法とは、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、ランダムに１個の復号鍵を選択することであるように構成してもよい。

【０００９】ここで、前記第１の所定の方法とは、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、一様にランダムに１個の復号鍵を選択することであるように構成してもよい。

【００１０】ここで、前記Ｍ種類の暗号装置のそれぞれは、前記鍵管理装置から配布された１つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する第２暗号鍵記憶手段と、スクランブルキーを生成するスクランブルキー生成手段と、外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、前記第２暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるＮ個の暗号鍵を用いて、第２の所定の方法により、前記スクランブルキーを順次暗号化し、Ｎ個の暗号化スクランブルキーを生成する鍵暗号化手段と、前記生成された暗号化デジタルデータと前記生成されたＮ個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備えるように構成してもよい。

【００１１】ここで、前記第２の所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであるように構成してもよい。

【００１２】ここで、前記第２の所定の方法とは、前記スクランブルキーを暗号化してＮ個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化してＮ個の暗号化固定情報を生成することであり、前記媒体書込手段は、暗号化デジタルデータとＮ個の暗号化スクランブルキーとＮ個の暗号化固定情報とを配布媒体に書き込むように構成してもよい。

【００１３】ここで、前記復号選択手段は、前記復号鍵セットから復号鍵を順次読み出す第１復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第１復号文生成手段と、前記第１の所定の基準により、復号

文が正しく復号されているかどうかを検査する第１復号文検査手段と、前記復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第１復号鍵読出手段、前記第１復号文生成手段、前記第１復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第３繰返制御手段と、前記復号文検査手段により正しく復号されたと検査された際に用いられた復号鍵を出力する鍵出力手段とを備えるように構成してもよい。

【００１４】ここで、前記第１の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであるように構成してもよい。

【００１５】ここで、前記配布媒体は、さらに、前記暗号鍵セットに含まれるＮ個の暗号鍵を用いて固定値からなる固定情報が暗号化されたＮ個の暗号化固定情報を含み、前記鍵管理装置は、さらに、Ｎ個の暗号化固定情報を読み出す暗号化固定情報読出手段と、前記Ｎ個の復号鍵セットを用いて、前記読み出したＮ個の暗号化固定情報をそれぞれ復号する暗号化固定情報復号手段とを含み、前記第１の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであるように構成してもよい。

【００１６】ここで、前記Ｎ種類の復号装置のそれぞれは、前記鍵管理装置から識別番号を受信し、受信した識別番号を記憶する識別番号記憶手段と、前記鍵管理装置から配布された１つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する第２復号鍵記憶手段と、前記配布媒体から前記受信した識別番号により識別される１つの暗号化スクランブルキーを読み出す第２暗号文読出手段と、前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、前記第２復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す第２復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第２復号文生成手段と、前記第１の所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文をスクランブルキーとする第２復号文検査手段と、復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第２復号鍵読出手段、前記第２復号文生成手段、前記第２復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第４繰返制御手段と、前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えるように構成してもよい。

【００１７】ここで、前記第１の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであるように構成してもよい。

【００１８】ここで、前記配布媒体は、さらに、前記暗号鍵セットに含まれるＮ個の暗号鍵を用いて固定値からなる固定情報が暗号化されたＮ個の暗号化固定情報を含み、前記復号装置は、さらに、前記識別番号により識別される１つの暗号化固定情報を読み出す暗号化固定情報読出手段と、前記復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を復号する暗号化固定情報復号手段とを備え、前記第１の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであるように構成してもよい。

【００１９】

【発明の実施の形態】本発明に係る１つの実施の形態としての暗号システム１０について説明する。

１．暗号システム１０の構成

本発明に係る１つの実施の形態としての暗号システム１０の構成を示すブロック図を図１に示す。暗号システム１０は、この図に示すように、１つの鍵管理装置１００、Ｍ種類の暗号装置２００、２０１、・・・、２０２、Ｎ種類の復号装置３００、３０１、・・・、３０２から構成される。ここで、Ｍ及びＮは、２以上の整数である。

【００２０】鍵管理装置１００は、Ｍ種類の暗号鍵セット記録媒体２１を生成し、Ｍ種類の暗号鍵セット記録媒体２１は、それぞれＭ種類の暗号装置２００、２０１、・・・、２０２に配布される。また、鍵管理装置１００は、Ｎ種類の復号鍵セット記録媒体２２を生成し、Ｎ種類の復号鍵セット記録媒体２２は、それぞれＮ種類の復号装置３００、３０１、・・・、３０２に配布される。Ｍ種類の暗号装置２００、２０１、・・・、２０２のそれぞれは、デジタル著作物記録媒体３１に記録されているデジタル著作物を暗号化し、暗号化したデジタル著作物をＭ種類の配布媒体４０、４１、・・・、４２に書き込む。Ｎ種類の復号装置３００、３０１、・・・、３０２のそれぞれは、Ｍ種類の配布媒体４０、４１、・・・、４２のいずれかから暗号化されたデジタル著作物を読み出し、復号する。また、鍵管理装置１００は、配布媒体５０を生産した暗号装置の種類を特定する。以下に、上記の各装置の構成について詳細に説明する。

【００２１】１．１　鍵管理装置１００の構成

鍵管理装置１００は、図２に示すように、復号鍵セット配布部１１１、復号鍵テーブル１１２、暗号鍵生成部１１３、暗号鍵テーブル１１４、暗号鍵生成制御部１１５、暗号鍵セット配布部１１６、識別番号配布部１２１、識別番号記憶部１２２、復号選択制御部１３１、復号鍵セット読出部１３２、暗号文読出部１３３、復号選択部１３４、鍵パターン検出部１３５、暗号装置管理処理部１３６から構成され、復号選択部１３４は、図３に示すように、復号鍵読出部１４１、復号制御部１４２、

復号文生成部１４３、復号文検査部１４４、鍵出力部１４５から構成される。鍵管理装置１００は、２つの機能を有する。第１の機能は、暗号鍵、復号鍵、識別番号の生成と配布である。第２の機能は、配布媒体を生産した暗号装置の種類の特定である。

【００２２】１．１．１　復号鍵テーブル１１２

復号鍵テーブル１１２は、図４に示すように、あらかじめＮ個の復号鍵セット４００、４０１、・・・、４０２を有し、Ｎ個の復号鍵セット４００、４０１、・・・、４０２のそれぞれは、Ｒ個の鍵を含む。これらの鍵は、暗号文を復号する際に用いられるものである。ここで、Ｒは２以上の整数である。前記復号鍵の長さは、それぞれ１２８ビットである。Ｎ個の復号鍵セット４００、４０１、・・・、４０２は、それぞれ１、２、・・・、Ｎからなる番号で識別される。また、Ｎ個の復号鍵セット４００、４０１、・・・、４０２のそれぞれに含まれるＲ個の鍵は、それぞれ１、２、・・・、ｒからなる番号で識別される。ここで、ｉ番めの復号鍵セットに含まれるｊ番目の鍵をK_{ij}と表す。Ｎ個の復号鍵セットは、それぞれＮ種類の復号装置３００、３０１、・・・、３０２に割り当てられる。復号鍵テーブル１１２の一例を図５に示す。図５に示す復号鍵テーブル５１０は、５個の復号鍵セット５００、５０１、５０２、５０３、５０４を有しており、５個の復号鍵セット５００、５０１、５０２、５０３、５０４のそれぞれは、２個の鍵を含む。復号鍵セット５００、５０１、５０２、５０３、５０４は、それぞれ５種類の復号装置D_1、D_2、D_3、D_4、D_5に割り当てられる。

【００２３】１．１．２　暗号鍵生成制御部１１５

暗号鍵生成制御部１１５は、暗号鍵生成部１１３に対して、Ｍ個の暗号鍵セット４２０、４２１、・・・、４２２を順次生成するように制御する。Ｍ個の暗号鍵セット４２０、４２１、・・・、４２２は、それぞれＮ個の鍵を含む。具体的には、暗号鍵生成制御部１１５は、生成された暗号鍵セットの番号を１からＭまで、１ずつ順に加算して得られる値を暗号鍵生成部１１３へ出力する。Ｍ個の暗号鍵セット４２０、４２１、・・・、４２２は、それぞれ１、２、・・・、Ｍからなる番号で識別される。また、Ｍ個の暗号鍵セット４２０、４２１、・・・、４２２のそれぞれに含まれるＮ個の鍵は、それぞれ１、２、・・・、Ｎからなる番号で識別される。

【００２４】１．１．３　暗号鍵生成部１１３

暗号鍵生成部１１３は、暗号鍵生成制御部１１５の制御のもとに、暗号鍵生成制御部１１５から番号１を受け取ると、１番目の暗号鍵セット４２０を、次に示すようにして生成する。暗号鍵生成部１１３は、復号鍵テーブル１１２を構成する１番目の復号鍵セット４００に含まれるＲ個の鍵から、１個の鍵をランダムに選択し、選択した１個の鍵を１番目の鍵として暗号鍵テーブル１１４の１番目の暗号鍵セット４２０に書き込む。次に、暗号鍵生成部１１３は、復号鍵テーブル１１２を構成する２番目の復号鍵セット４０１に含まれるＲ個の鍵から、１個の鍵をランダムに選択し、選択した１個の鍵を２番目の鍵として暗号鍵テーブル１１４の１番目の暗号鍵セット４２０に書き込む。暗号鍵生成部１１３は、以下同様にして、３番目以降の復号鍵セットからランダムに各１個の鍵を選択し、３番目以降の鍵として暗号鍵セット４２０に書き込むことを繰り返す。こうして、暗号鍵生成部１１３は、Ｎ個の鍵を含む暗号鍵セット４２０を、暗号鍵テーブル１１４内に生成する。暗号鍵生成部１１３は、同様にして、暗号鍵生成制御部１１５の制御のもとに、暗号鍵生成制御部１１５から番号２から番号Ｍを受け取ると、２番目からＭ番目までの暗号鍵セットを生成し、暗号鍵テーブル１１４に書き込む。

【００２５】１．１．４　暗号鍵テーブル１１４

暗号鍵テーブル１１４は、図４に示すように、Ｍ個の暗号鍵セット４２０、４２１、・・・、４２２を有し、Ｍ個の暗号鍵セット４２０、４２１、・・・、４２２のそれぞれは、Ｎ個の鍵を含む。これらの鍵は、平文を暗号化する際に用いられるものである。前記暗号鍵の長さは、それぞれ１２８ビットである。Ｍ個の暗号鍵セットは、それぞれＭ種類の暗号装置２００、２０１、・・・、２０２に割り当てられる。暗号鍵テーブル１１４の一例を図６に示す。図６に示す暗号鍵テーブル６１０は、４個の暗号鍵セット６００、６０１、６０２、６０３を有しており、４個の暗号鍵セット６００、６０１、６０２、６０３は、それぞれ５個の鍵を含む。暗号鍵セット６００、６０１、６０２、６０３は、それぞれ４種類の暗号装置E_1、E_2、E_3、E_4に割り当てられる。

【００２６】１．１．５　復号鍵セット配布部１１１

復号鍵セット配布部１１１は、復号鍵テーブル１１２から１番目の復号鍵セット４００を読み出し、読み出した１番目の復号鍵セット４００を１番目の復号鍵セット記録媒体に書き込む。次に、復号鍵セット配布部１１１は、復号鍵テーブル１１２から２番目の復号鍵セット４０１を読み出し、読み出した２番目の復号鍵セット４０１を２番目の復号鍵セット記録媒体に書き込む。復号鍵セット配布部１１１は、同様にして、３番目からＮ番目までの復号鍵セットの読み出しと３番目からＮ番目までの復号鍵セット記録媒体へ書き込むとを繰り返す。こうして、復号鍵セット配布部１１１は、復号鍵テーブル１１２のＮ個の復号鍵セットのそれぞれをＮ個の復号鍵セット記録媒体へ書き込む。

【００２７】１．１．６　暗号鍵セット配布部１１６

暗号鍵セット配布部１１６は、暗号鍵テーブル１１４から１番目の暗号鍵セット４２０を読み出し、読み出した１番目の暗号鍵セット４２０を１番目の暗号鍵セット記録媒体に書き込む。次に、暗号鍵セット配布部１１６は、暗号鍵テーブル１１４から２番目の暗号鍵セット４

２１を読み出し、読み出した２番目の暗号鍵セット４２１を２番目の暗号鍵セット記録媒体に書き込む。暗号鍵セット配布部１１６は、同様にして、３番目からM番目までの暗号鍵セットの読み出しと３番目からM番目までの暗号鍵セット記録媒体への書き込みとを繰り返す。こうして、暗号鍵セット配布部１１６は、暗号鍵テーブル１１４のM個の暗号鍵セットのそれぞれをM個の暗号鍵セット記録媒体へ書き込む。

【００２８】１．１．７　識別番号記憶部１２２

識別番号記憶部１２２は、N個の識別番号を記憶している。N個の識別番号は、N種類の復号装置３００、３０１、・・・、３０２にそれぞれ対応している。識別番号は、各復号装置が配布媒体に書き込まれている暗号化デジタル著作物を復号する際に、配布媒体に書き込まれているN個の暗号化スクランブルキーの中から当該復号装置に対応した１つの暗号化スクランブルキーを識別するために用いられる。

【００２９】１．１．８　識別番号配布部１２１

識別番号配布部１２１は、N個の復号鍵セット記録媒体毎に、各復号装置に対応する識別番号を、識別番号記憶部１２２より、読み出し、読み出した識別番号を対応する復号鍵セット記録媒体に書き込む。

【００３０】１．１．９　復号選択制御部１３１

復号選択制御部１３１は、配布媒体５０からN個の暗号化スクランブルキーの読み出しが終了するまで、暗号文読出部１３３と、復号鍵セット読出部１３２と、復号選択部１３４とに対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とをN回繰り返し行うように、制御する。なお、暗号化スクランブルキーについては、後述する。具体的には、復号選択制御部１３１は、番号１の暗号化スクランブルキーを読み出すように、暗号文読出部１３３に対して制御し、次に、番号１の復号鍵セットを読み出すように、復号鍵セット読出部１３２に対して制御し、次に、番号１の復号鍵セットに含まれるR個の鍵を用いて、前記読み出した番号１の暗号化スクランブルキーを復号し、第１の所定の基準により、正しく暗号化スクランブルキーを復号する鍵を、前記R個の鍵の中から１つ選択するように、復号選択部１３４に対して制御する。続けて、復号選択制御部１３１は、番号２から番号Nについて、上記の制御を繰り返す。上記の繰り返しが終了すると、N個の復号されたスクランブルキーを含む復号文が復号される際に用いられたN個の鍵のセットが選択される。

【００３１】１．１．１０　暗号文読出部１３３

暗号文読出部１３３は、復号選択制御部１３１の制御の元に、暗号化スクランブルキーの番号の指定を受けて、配布媒体５０から、前記指定された番号により特定される一つの暗号化スクランブルキーを読み出す。

【００３２】１．１．１１　復号鍵セット読出部１３２

復号鍵セット読出部１３２は、復号選択制御部１３１の制御の元に、復号鍵セットの番号の指定を受けて、復号鍵テーブル１１２から、前記指定された番号により特定される一つの復号鍵セットを読み出す。

【００３３】１．１．１２　復号選択部１３４

復号選択部１３４は、復号選択制御部１３１の制御の元に、復号鍵セット読出部１３２により読み出された１つの復号鍵セットに含まれるR個の鍵を用いて、暗号文読出部１３３により読み出された暗号化スクランブルキーを復号し、第１の所定の基準により、正しく暗号化スクランブルキーを復号する鍵を、前記R個の鍵の中から１つ選択する。復号選択部１３４を構成する復号鍵読出部１４１、復号制御部１４２、復号文生成部１４３、復号文検査部１４４、鍵出力部１４５について、以下に説明する。

【００３４】（１）　復号鍵読出部１４１

復号鍵読出部１４１は、復号制御部１４２の制御の元に、復号鍵セット読出部１３２により読み出された復号鍵セットから、復号制御部１４２から読み出す鍵の番号の指定を受けて、指定された番号により特定される１つの鍵を読み出す。

【００３５】（２）　復号文生成部１４３

復号文生成部１４３は、復号制御部１４２の制御の元に、復号鍵読出部１４１により読み出された鍵を用いて、前記暗号文読出部１３３により読み出された暗号化スクランブルキーを含む暗号文を復号し、スクランブルキーを含む復号文を生成する。なお、復号文生成部１４３の構成は、後述する復号文生成部３０６と同様であるので、説明を省略する。

【００３６】（３）　復号文検査部１４４

復号文検査部１４４は、復号制御部１４２の制御の元に、復号文生成部１４３により生成されたスクランブルキーを含む復号文が、第１の所定の基準により、正しく復号されているかどうかを検査する。ここで、第１の所定の基準とは、図７に示すように、スクランブルキーを含む復号文の前半の６４ビットに固定値からなる固定情報が含まれることである。前記固定値は、６４ビットの連続する０である。スクランブルキーを含む復号文の後半の６４ビットはスクランブルキーである。すなわち、復号文検査部１４４は、生成されたスクランブルキーを含む復号文の前半の６４ビットが連続する０である場合には、復号鍵読出部１４１により読み出され、復号に用いられた鍵が正しく、正しくスクランブルキーが復号されたものとみなす。生成されたスクランブルキーを含む復号文の前半の６４ビットが連続する０以外である場合には、復号鍵読出部１４１により読み出され、復号に用いられた鍵が誤っていたものとみなす。

【００３７】（４）　復号制御部１４２

復号制御部１４２は、復号鍵セット読出部１３２により読み出された復号鍵セットからR個の鍵の読出しが終了

するまで、復号鍵読出部１４１、復号文生成部１４３、復号文検査部１４４に対して、鍵の読出しと、暗号化スクランブルキーの復号と、復号されたスクランブルキーの検査とをＲ回繰り返し行うように制御する。具体的には、復号制御部１４２は、復号鍵セット読出部１３２により読み出された復号鍵セットから、番号１の鍵を読み出すように、復号鍵読出部１４１に対して制御し、次に、番号１の鍵を用いて、暗号文読出部１３３により読み出された暗号化スクランブルキーを復号するように、復号文生成部１４３に対して制御し、次に、復号文生成部１４３により生成されたスクランブルキーが正しく復号されているかどうかを検査するように、復号文検査部１４４を制御する。復号選択制御部１３１は、番号２から番号Ｒについて、上記の制御を繰り返す。上記の繰り返しが終了すると、復号鍵読出部１４１により読み出され、正しく復号された１個のスクランブルキーが復号される際に用いられた１個の鍵が選択される。

【００３８】（５）　鍵出力部１４５

鍵出力部１４５は、前記復号文検査部１４４により正しく復号されたと検査された１個のスクランブルキーを復号する際に用いられた１個の鍵を、鍵パターン検出部１３５へ出力する。

【００３９】１．１．１３　鍵パターン検出部１３５

鍵パターン検出部１３５は、暗号鍵テーブル１１４に記憶されているＭ個の暗号鍵セット４２０、４２１、・・・、４２２から、復号選択制御部１３１によって前記選択されたＮ個の鍵のセットと一致する１つの暗号鍵セットを検出し、検出された暗号鍵セットの番号を暗号装置管理処理部１３６へ出力する。この番号により特定される暗号装置により、配布媒体５０が生産されたものと分かる。

【００４０】１．１．１４　暗号装置管理処理部１３６

暗号装置管理処理部１３６は、鍵パターン検出部１３５より、検出された暗号鍵セットの番号を受け取る。暗号装置管理処理部１３６は、Ｍ種類の暗号装置毎に、暗号装置の番号と、暗号装置の名称と、暗号装置の製造メーカーとを記憶している。暗号装置管理処理部１３６は、前記受け取った番号を基にして、前記記憶内容より、暗号装置の名称と、暗号装置の製造メーカーとを検索し、検索された暗号装置の名称と、暗号装置の製造メーカーとを表示する。

【００４１】１．２　鍵管理装置１００の動作

ここでは、鍵管理装置１００の鍵生成と鍵の配布の動作と、鍵管理装置１００の暗号装置を特定する動作について説明する。

【００４２】１．２．１　鍵管理装置１００の鍵生成と鍵の配布の動作

鍵管理装置１００の鍵生成と鍵の配布の動作について、図８に示すフローチャートを用いて説明する。暗号鍵生成制御部１１５は、ｉの値を１からＭまで１ずつ増加させて変化させて、暗号鍵生成部１１３に対して暗号鍵セットの生成制御を繰り返す（ステップＳ８０１～ステップＳ８０６）。ここで、ｉは、正の整数の値をとるカウンタである。暗号鍵生成部１１３は、ｊの値を１からＮまで１ずつ増加させて変化させて（ステップＳ８０２～ステップＳ８０５）、復号鍵セットに含まれるＲ個の鍵から、１個の鍵をランダムに選択し、（ステップＳ８０３）、選択した１個の鍵をｊ番目の鍵として暗号鍵テーブル１１４のｉ番目の暗号鍵セットに書き込む（ステップＳ８０４）動作をＮ回繰り返す。ここで、ｊは、正の整数の値をとるカウンタである。次に、暗号鍵セット配布部１１６は、暗号鍵テーブル１１４のＭ個の暗号鍵セットのそれぞれをＭ個の暗号鍵セット記録媒体へ書き込み（ステップＳ８０７～ステップＳ８１０）、復号鍵セット配布部１１１は、復号鍵テーブル１１２のＮ個の復号鍵セット及び識別番号記憶部のＮ個の識別番号のそれぞれをＮ個の復号鍵セット記録媒体へ書き込む（ステップＳ８１１～ステップＳ８１３）。

【００４３】１．２．２　鍵管理装置１００の暗号装置を特定する動作

鍵管理装置１００の暗号装置を特定する動作について、図９に示すフローチャートを用いて説明する。復号選択制御部１３１は、ｎを１からＮまで、１ずつ加算することにより、配布媒体５０からＮ個の暗号化スクランブルキーの読み出しが終了するまで、暗号文読出部１３３と、復号鍵セット読出部１３２と、復号選択部１３４とに対して、暗号化スクランブルキーの読み出し（ステップＳ９０２）と、復号鍵セットの読み出し（ステップＳ９０３）と、読み出した暗号化スクランブルキーの復号と鍵の選択（ステップＳ９０４）とをＮ回繰り返し行うように、制御する（ステップＳ９０１～ステップＳ９１０）。ここで、ｎは、正の整数の値をとるカウンタである。上記の繰り返しが終了すると、Ｎ個の復号されたスクランブルキーを含む復号文が復号される際に用いられたＮ個の鍵のセットが選択される。ここで、暗号化スクランブルキーの復号（ステップＳ９０４）では、復号制御部１４２は、ｒを１からＲまで、１ずつ加算することにより、復号鍵セット読出部１３２により読み出された復号鍵セットからＲ個の第１鍵の読出しが終了するまで、復号鍵読出部１４１、復号文生成部１４３、復号文検査部１４４に対して、鍵の読出し（ステップＳ９０６）と、暗号化スクランブルキーの復号（ステップＳ９０７）と、復号されたスクランブルキーの検査（ステップＳ９０８）とをＲ回繰り返し行うように制御する。ここで、ｒは、正の整数の値をとるカウンタである。

【００４４】次に、鍵パターン検出部１３５は、ｍを１からＭまで、１ずつ加算することにより、暗号鍵テーブル１１４に記憶されているＭ個の暗号鍵セット４２０、４２１、・・・、４２２から、前記選択されたＮ個の鍵のセットと一致する１つの暗号鍵セットを検出し（ステ

ップＳ９１１～ステップＳ９１３）、検出された暗号鍵セットの番号を暗号装置管理処理部１３６へ出力し、暗号装置管理処理部１３６は、前記受け取った番号を基にして、暗号装置の名称と、暗号装置の製造メーカーとを表示する（ステップＳ９１４）。ここで、ｍは、正の整数の値をとるカウンタである。

【００４５】１．３　暗号装置２００の構成

ここでは、暗号装置２００の構成について説明する。なお、暗号装置２０１、・・・、２０２については同様の構成であるので説明を省略する。暗号装置２００は、図１０に示すように、暗号鍵記憶部２０５、デジタルデータ暗号化部２０２、スクランブルキー生成部２０３、鍵暗号化部２０４から構成される。

【００４６】１．３．１　暗号鍵記憶部２０５

暗号鍵記憶部２０５は、配布された暗号鍵セット記録媒体２１から、Ｎ個の鍵を含む１つの暗号鍵セットを読み出し、読み出した１つの暗号鍵セットを記憶する。ここで、Ｎ個の鍵はそれぞれ１２８ビットの長さである。

【００４７】１．３．２　スクランブルキー生成部２０３

スクランブルキー生成部２０３は、乱数を用いて、６４ビットのスクランブルキーを生成し、６４ビットの連続する０と前記生成された６４ビットのスクランブルキーとを結合し、結合された６４ビットの連続する０と前記生成された６４ビットのスクランブルキーとを鍵暗号化部２０４へ出力する。また、スクランブルキー生成部２０３は、前記生成された６４ビットのスクランブルキーをデジタルデータ暗号化部２０２へ出力する。

【００４８】１．３．３　鍵暗号化部２０４

鍵暗号化部２０４は、図１１に示すように、分解部２１１、ＤＥＳ暗号化部２１２、２１３、分解部２１４、結合部２１５から構成される。

【００４９】（１）分解部２１１

分解部２１１は、スクランブルキー生成部２０３から出力された、結合された６４ビットの連続する０と６４ビットのスクランブルキーとを、６４ビットの連続する０と６４ビットのスクランブルキーとに分解し、６４ビットの連続する０をＤＥＳ暗号化部２１２へ出力し、６４ビットのスクランブルキーをＤＥＳ暗号化部２１３へ出力する。

【００５０】（２）分解部２１４

分解部２１４は、暗号鍵記憶部２０５から、Ｎ個の鍵を、Ｎ回繰り返して順次読み出し、読み出した各鍵を前半の６４ビットと、後半の６４ビットに分解し、前半の６４ビットをＤＥＳ暗号化部２１２へ出力し、後半の６４ビットをＤＥＳ暗号化部２１３へ出力する。

【００５１】（３）ＤＥＳ暗号化部２１２

ＤＥＳ暗号化部２１２は、分解部２１４から出力された６４ビットの鍵を用いて、データ暗号化規格（ＤＥＳ、Ｄａｔｅ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）

により規格されるＤＥＳ暗号化アルゴリズムにより、分解部２１１から出力された６４ビットの連続する０を暗号化して６４ビットの暗号文を生成し、生成された６４ビットの暗号文を結合部２１５へ出力する。ＤＥＳについては、公知であるので、説明を省略する。

【００５２】（４）ＤＥＳ暗号化部２１３

ＤＥＳ暗号化部２１３は、分解部２１４から出力された６４ビットの鍵を用いて、ＤＥＳ暗号化アルゴリズムにより、分解部２１１から出力された６４ビットのスクランブルキーを暗号化し、６４ビットの暗号文を生成し、生成された６４ビットの暗号文を結合部２１５へ出力する。

【００５３】（５）結合部２１５

結合部２１５は、ＤＥＳ暗号化部２１２から出力された６４ビットの暗号文と、ＤＥＳ暗号化部２１３から出力された６４ビットの暗号文とをこの順で結合し、結合されて生成された１２８ビットの暗号文を配布媒体４０に書き込む。このようにして、Ｎ個の暗号文が配布媒体４０に書き込まれる。ここで、前記１２８ビットの暗号文を暗号化スクランブルキーと呼ぶ。

【００５４】１．３．４　デジタルデータ暗号化部２０２

デジタルデータ暗号化部２０２は、デジタル著作物記録媒体３１に記録されているデジタル著作物を読み出し、スクランブルキー生成部２０３から出力された６４ビットのスクランブルキーを用いて、ＤＥＳ暗号化アルゴリズムにより、前記読み出したデジタル著作物を暗号化して、暗号化デジタル著作物を生成し、生成した暗号化デジタル著作物を配布媒体４０に書き込む。

【００５５】デジタルデータ暗号化部２０２の動作について、図１２に示すフローチャートを用いて説明する。デジタルデータ暗号化部２０２は、スクランブルキー生成部２０３から出力された６４ビットのスクランブルキーを受け取り（ステップＳ１２０１）、デジタル著作物記録媒体３１に記録されているデジタル著作物から６４ビット分のデジタルデータを読み出し（ステップＳ１２０２）、デジタルデータの読み出しが終了していれば（ステップＳ１２０３）、処理を終了し、デジタルデータの読み出しが終了していなければ（ステップＳ１２０３）、前記６４ビットのスクランブルキーを用いて、ＤＥＳ暗号化アルゴリズムにより、読み出した６４ビット分のデジタルデータを暗号化して、６４ビット分の暗号化デジタルデータを生成し（ステップＳ１２０４）、生成した暗号化デジタルデータを配布媒体４０に書き込む（ステップＳ１２０５）。次に、再度ステップＳ１２０２に制御を戻し、デジタルデータの読み出しが終了するまで、デジタルデータの読み出しとデジタルデータの暗号化と暗号化デジタルデータの配布媒体への書き込みを繰り返す。

【００５６】１．４　暗号装置２００の動作

ここでは、暗号装置２００の動作について、図１３に示すフローチャートを用いて説明する。なお、暗号装置２０１、・・・、２０２についても同様であるので、説明は省略する。暗号鍵記憶部２０５は、配布された暗号鍵セット記録媒体２１から、Ｎ個の鍵を含む１つの暗号鍵セットを読み出し、読み出した１つの暗号鍵セット４２０を記憶すする（ステップＳ１３１１）。スクランブルキー生成部２０３は、乱数を用いて、６４ビットのスクランブルキーを生成し、６４ビットの連続する０と前記生成された６４ビットのスクランブルキーとを結合し、結合された６４ビットの連続する０と前記生成された６４ビットのスクランブルキーとを鍵暗号化部２０４へ出力し、前記生成された６４ビットのスクランブルキーをデジタルデータ暗号化部２０２へ出力する（ステップＳ１３１２）。

【００５７】分解部２１１は、スクランブルキー生成部２０３から出力された、結合された６４ビットの連続する０と６４ビットのスクランブルキーとを、６４ビットの連続する０と６４ビットのスクランブルキーとに分解し、６４ビットの連続する０をＤＥＳ暗号化部２１２へ出力し、６４ビットのスクランブルキーをＤＥＳ暗号化部２１３へ出力し、分解部２１４は、暗号鍵記憶部２０５から、Ｎ個の鍵を、Ｎ回繰り返して順次読み出し、読み出した各鍵を前半の６４ビットと、後半の６４ビットに分解し、前半の６４ビットをＤＥＳ暗号化部２１２へ出力し、後半の６４ビットをＤＥＳ暗号化部２１３へ出力し、ＤＥＳ暗号化部２１２は、分解部２１４から出力された６４ビットの鍵を用いて、データ暗号化規格（ＤＥＳ、Ｄａｔｅ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）により規格されるＤＥＳ暗号化アルゴリズムにより、分解部２１１から出力された６４ビットの連続する０を暗号化して６４ビットの暗号文を生成し、生成された６４ビットの暗号文を結合部２１５へ出力し、ＤＥＳ暗号化部２１３は、分解部２１４から出力された６４ビットの鍵を用いて、ＤＥＳ暗号化アルゴリズムにより、分解部２１１から出力された６４ビットのスクランブルキーを暗号化し、６４ビットの暗号文を生成し、生成された６４ビットの暗号文を結合部２１５へ出力し、結合部２１５は、ＤＥＳ暗号化部２１２から出力された６４ビットの暗号文と、ＤＥＳ暗号化部２１３から出力された６４ビットの暗号文とをこの順で結合し、結合されて生成された１２８ビットの暗号文を配布媒体４０に書き込む。このようにして、Ｎ個の暗号化スクランブルキーが配布媒体４０に書き込まれる（ステップＳ１３１３）。

【００５８】デジタルデータ暗号化部２０２は、デジタル著作物記録媒体３１に記録されているデジタル著作物を読み出し、スクランブルキー生成部２０３から出力された６４ビットのスクランブルキーを用いて、ＤＥＳ暗号化アルゴリズムにより、前記読み出したデジタル著作物を暗号化して、暗号化デジタル著作物を生成し、生成した暗号化デジタル著作物を配布媒体４０に書き込む（ステップＳ１３１４）。このようにして、図１４に示すように、配布媒体４０には、Ｎ個の暗号化スクランブルキー１３０１、１３０２、・・・、１３０３と暗号化デジタル著作物１３０４とが書き込まれる。

【００５９】１．５　復号装置３００の構成

ここでは、復号装置３００の構成について説明する。なお、復号装置３０１、・・・、３０２については同様の構成であるので説明を省略する。復号装置３００は、図１５に示すように、識別番号記憶部３１１、復号鍵記憶部３１２、復号鍵読出部３０３、復号検査制御部３０４、暗号文読出部３０５、復号文生成部３０６、復号文検査部３０７、デジタルデータ読出部３０８、デジタルデータ復号部３０９、表示部３１０から構成される。

【００６０】１．５．１　識別番号記憶部３１１

識別番号記憶部３１１は、復号鍵セット記録媒体２２から、識別番号を読み出し、読み出した識別番号を記憶する。

【００６１】１．５．２　復号鍵記憶部３１２

復号鍵記憶部３１２は、復号鍵セット記録媒体２２から、Ｒ個の鍵を含む復号鍵セットを読み出し、読み出した復号鍵セットを記憶する。

【００６２】１．５．３　暗号文読出部３０５

暗号文読出部３０５は、識別番号記憶部３１１に記憶されている識別番号を読み出し、読み出した識別番号により識別される１つの暗号化スクランブルキーを配布媒体から読み出し、読み出した１つの暗号化スクランブルキーを復号文生成部３０６へ出力する。

【００６３】１．５．４　復号検査制御部３０４

復号検査制御部３０４は、復号鍵セットからＲ個の鍵の読み出しが終了するまで、復号鍵読出部３０３、復号文生成部３０６、復号文検査部３０７に対して、１つの鍵の読み出しと、暗号化スクランブルキーの復号と、暗号化スクランブルキーを復号して得られた復号文の検査とをＲ回繰り返し行うように制御する。具体的には、復号検査制御部３０４は、復号鍵セットから番号１の鍵を読み出すように、復号鍵読出部３０３に対して制御する。次に、読み出された番号１の鍵を用いて、暗号化スクランブルキーを復号して復号文を生成するように、復号文生成部３０６に対して制御する。さらに、生成された復号文を、前記第１の所定の基準により、正しく復号されているかどうかを検査するように、復号文検査部３０７に対して制御する。続けて、復号検査制御部３０４は、番号２から番号Ｒの鍵について、上記の制御を繰り返す。上記の繰り返しが終了すると、Ｒ個の鍵から、暗号化スクランブルキーを正しく復号する１つの鍵が選択される。

【００６４】１．５．５　復号鍵読出部３０３

復号鍵読出部３０３は、復号検査制御部３０４の制御の

元で、復号鍵記憶部３０２に記憶されている復号鍵セットの中から、復号検査制御部３０４により指定される番号の１つの鍵を読み出し、読み出した１つの鍵を復号文生成部３０６へ出力する。

【００６５】１．５．６　復号文生成部３０６

復号文生成部３０６は、図１６に示すように、分解部３２１、ＤＥＳ復号部３２２、ＤＥＳ復号部３２３、分解部３２４、結合部３２５から構成され、復号検査制御部３０４の制御の元に動作する。

【００６６】（１）分解部３２１

分解部３２１は、暗号文読出部３０５から出力される暗号化スクランブルキーを受け取る。この暗号化スクランブルキーは、１２８ビットの長さを有する。分解部３２１は、受け取った暗号化スクランブルキーを前半の６４ビットのデータと後半の６４ビットとのデータに分解し、前半の６４ビットのデータをＤＥＳ復号部３２２へ出力し、後半の６４ビットのデータをＤＥＳ復号部３２３へ出力する。

【００６７】（２）分解部３２４

分解部３２４は、復号鍵読出部３０３から出力される１つの鍵を受け取る。この１つの鍵は、１２８ビットの長さを有する。分解部３２４は、受け取った１つの鍵を前半の６４ビットのデータと後半の６４ビットとのデータに分解し、前半の６４ビットのデータをＤＥＳ復号部３２２へ出力し、後半の６４ビットのデータをＤＥＳ復号部３２３へ出力する。

【００６８】（３）ＤＥＳ復号部３２２

ＤＥＳ復号部３２２は、分解部３２４から出力された６４ビットの鍵を用いて、データ暗号化規格（ＤＥＳ、Ｄａｔｅ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）により規格されるＤＥＳ復号アルゴリズムにより、分解部３２１から出力された６４ビットのデータを暗号化して６４ビットの復号文を生成し、生成された６４ビットの復号文を結合部３２５へ出力する。

【００６９】（４）ＤＥＳ復号部３２３

ＤＥＳ復号部３２３は、分解部３２４から出力された６４ビットの鍵を用いて、ＤＥＳ復号アルゴリズムにより、分解部３２１から出力された前半６４ビットのデータを復号して６４ビットの復号文を生成し、生成された6-4ビットの復号文を結合部３２５へ出力する。

【００７０】（５）結合部３２５

結合部３２５は、ＤＥＳ復号部３２２から出力された後半６４ビットの復号文と、ＤＥＳ復号部３２３から出力された６４ビットの復号文とをこの順で結合し、結合されて生成された１２８ビットの復号文を復号文検査部３０７へ出力する。

【００７１】１．５．７　復号文検査部３０７

復号文検査部３０７は、復号検査制御部３０４の制御の元に、復号文生成部３０６により生成されたスクランブルキーを含む復号文が、前記第１の所定の基準により、

正しく復号されているかどうかを検査する。すなわち、復号文検査部３０７は、生成されたスクランブルキーを含む復号文の前半の６４ビットが連続する０である場合には、復号鍵読出部３０３により読み出され、復号に用いられた鍵が正しく、正しくスクランブルキーが復号されたものとみなす。生成されたスクランブルキーを含む復号文の前半の６４ビットが連続する０以外である場合には、復号鍵読出部３０３により読み出され、復号に用いられた鍵が誤っていたものとみなす。復号文検査部３０７は、正しく復号されたとする場合に、生成されたスクランブルキーを含む復号文の後半の６４ビットからなるスクランブルキーをデジタルデータ復号部３０９へ出力する。

【００７２】１．５．８　デジタルデータ読出部３０８

デジタルデータ読出部３０８は、配布媒体に記憶されている暗号化デジタル著作物を読み出し、読み出した暗号化デジタル著作物をデジタルデータ復号部３０９へ出力する。

【００７３】１．５．９　デジタルデータ復号部３０９

デジタルデータ復号部３０９は、復号文検査部３０７から受け取ったスクランブルキーを用いて、ＤＥＳ復号アルゴリズムにより、デジタルデータ読出部３０８により読み出された暗号化デジタル著作物を復号して、デジタル著作物を生成し、生成されたデジタル著作物を表示部３１０へ出力する。デジタルデータ復号部３０９の動作について、図１７に示すフローチャートを用いて説明する。

【００７４】デジタルデータ復号部３０９は、復号文検査部３０７から出力された６４ビットのスクランブルキーを受け取り（ステップＳ１７０１）、デジタルデータ読出部３０８により読み出された暗号化デジタル著作物から６４ビット分の暗号化デジタルデータを読み出し（ステップＳ１７０２）、暗号化デジタルデータの読み出しが終了していれば（ステップＳ１７０３）、処理を終了し、暗号化デジタルデータの読み出しが終了していなければ（ステップＳ１７０３）、前記６４ビットのスクランブルキーを用いて、ＤＥＳ復号アルゴリズムにより、読み出した６４ビット分の暗号化デジタルデータを復号して、６４ビット分のデジタルデータを生成し（ステップＳ１７０４）、生成したデジタルデータを表示部３１０へ出力する（ステップＳ１７０５）。次に、再度ステップＳ１７０２に制御を戻し、暗号化デジタルデータの読み出しが終了するまで、暗号化デジタルデータの読み出しと暗号化デジタルデータの復号化とデジタルデータの表示部３１０への出力を繰り返す。

【００７５】１．５．１０　表示部３１０

表示部３１０は、デジタルデータ復号部３０９から出力される６４ビットの復号されたデジタルデータを繰り返し受け取り、順次表示する。

【００７６】１．６　復号装置３００の動作

ここでは、復号装置３００の動作について、図１８に示すフローチャートを用いて説明する。なお、復号装置３０１、・・・、３０２についても、同様であるので、説明を省略する。識別番号記憶部３１１は、復号鍵セット記録媒体２２から、識別番号を読み出し、読み出した識別番号を記憶する（ステップＳ１８０１）。復号鍵記憶部３０２は、復号鍵セット記録媒体２２から、Ｒ個の鍵を含む復号鍵セットを読み出し、読み出した復号鍵セットを記憶する（ステップＳ１８０２）。

【００７７】暗号文読出部３０５は、識別番号記憶部３１１に記憶されている識別番号を読み出し、読み出した識別番号により識別される１つの暗号化スクランブルキーを配布媒体から読み出し、読み出した１つの暗号化スクランブルキーを復号文生成部３０６へ出力する（ステップＳ１８０３）。復号検査制御部３０４は、ｒを１からＲまで、１つずつ加算することにより、復号鍵セットからＲ個の鍵の読み出しが終了するまで、復号鍵読出部３０３、復号文生成部３０６、復号文検査部３０７に対して、１つの鍵の読み出し（ステップＳ１８０５）と、暗号化スクランブルキーの復号（ステップＳ１８０６）と、暗号化スクランブルキーを復号して得られた復号文の検査（ステップＳ１８０７～ステップＳ１８０９）とを繰り返し行うように制御する（ステップＳ１８０４～ステップＳ１８１０）。上記の繰り返しが終了すると、Ｒ個の鍵から、暗号化スクランブルキーを正しく復号する１つの鍵が選択され、復号文検査部３０７は、スクランブルキーをデジタルデータ復号部３０９へ出力する。次に、デジタルデータ読出部３０８は、暗号化デジタル著作物を読み出し、デジタルデータ復号部３０９は、復号文検査部３０７から受け取ったスクランブルキーを用いて、ＤＥＳ復号アルゴリズムにより、デジタルデータ読出部３０８により読み出された暗号化デジタル著作物を復号して、デジタル著作物を生成し、生成されたデジタル著作物を表示部３１０へ出力し（ステップＳ１８１１）、表示部３１０は、デジタルデータ復号部３０９から出力される６４ビットのデジタルデータを繰り返し受け取り、順次表示する（ステップＳ１８１２）。

【００７８】２．その他の実施の形態

なお、本発明を上記実施の形態に基づいて説明してきたが、本発明は上記実施の形態に限定されないのはもちろんである。すなわち、以下のような場合も本発明に含まれる。

（１）本実施の形態では、復号鍵候補の決定のために、６４ビットのスクランブルキーの先頭に６４ビットの連続する０を付加して暗号化し、復号時に先頭６４ビットが０であるかどうかを検査するとしているが、これに限定されるものではない。暗号装置において、６４ビットのスクランブルキーを暗号化し、引き続き、固定的な情報の暗号化を行ってＮ個の暗号化固定情報を生成し、復号装置においては、識別番号により識別される暗号化固定情報を復号して、その復号文が固定的な情報になるかどうかにより判断するとしてもよい。また、鍵管理装置においては、Ｎ個の暗号化固定情報を復号して、その復号文が固定的な情報になるかどうかにより判断するとしてもよい。

【００７９】（２）暗号鍵生成部１１３は、復号鍵セットに含まれるＲ個の鍵から、１個の鍵をランダムに選択し、選択した１個の鍵を暗号鍵テーブル１１４の暗号鍵セットに書き込むとしているが、暗号鍵生成部１１３は、復号鍵セットに含まれるＲ個の鍵から、一様に１個の鍵をランダムに選択し、選択した１個の鍵を暗号鍵テーブル１１４の暗号鍵セットに書き込むとしてもよい。ここで、一様に１個の鍵Ｋをランダムに選択するとは、Ｋを確率変数とすると、Ｋのとり得る範囲内で、確率密度関数ｆ（Ｋ）＝一定値を満たすように、Ｋをランダムに選択することを言う。

【００８０】（３）鍵管理装置１００は、暗号鍵セット記録媒体２１を各暗号装置に配布し、復号鍵セット記録媒体２２を各復号装置に配布するとしているが、前記記録媒体を配布する代わりに、鍵管理装置１００と各暗号装置を通信回線で結び、暗号鍵セット記録媒体２１に記録されている情報を前記通信回線を経由して、鍵管理装置１００から各暗号装置に送信するようにし、また、鍵管理装置１００と各復号装置を通信回線で結び、復号鍵セット記録媒体２２に記録されている情報を前記通信回線を経由して、鍵管理装置１００から各復号装置に送信するようにしてもよい。

【００８１】（４）本実施の形態では、ＤＥＳを使用しているが、他の暗号アルゴリズムを使用してもよい。

【００８２】

【発明の効果】上記に説明するように、本発明は、１台の鍵管理装置と、Ｍ（Ｍは２以上の整数）種類の暗号装置と、Ｎ（Ｎは２以上の整数）種類の復号装置とからなる暗号システムであって、前記鍵管理装置は、復号鍵セットをＮ個記憶し、暗号鍵セットをＭ個記憶し、Ｎ個の識別番号を記憶し、前記Ｍ個の暗号鍵セットをそれぞれ前記Ｍ種類の暗号装置に配布し、前記Ｎ個の復号鍵セットをそれぞれ前記Ｎ種類の復号装置に配布し、前記Ｎ個の識別番号をそれぞれ前記Ｎ種類の復号装置に配布し、前記暗号鍵セットはＮ個の暗号鍵からなり、前記復号鍵セットは所定数の復号鍵からなり、前記Ｍ種類の暗号装置のそれぞれは、デジタルデータをスクランブルキーを用いて暗号化して暗号化デジタルデータを生成し、前記配布された暗号鍵セットを用いて前記スクランブルキーを暗号化してＮ個の暗号化スクランブルキーを生成し、前記暗号化デジタルデータと前記Ｎ個の暗号化スクランブルキーとを配布媒体に書き込み、前記Ｎ種類の復号装置のそれぞれは、前記配布された復号鍵セットに含まれる前記所定数の復号鍵を用いて、前記配布媒体に含まれ前記配布された識別番号により特定される１つの暗号化

スクランブルキーを順次復号し、第１の所定の基準により正しく復号されたスクランブルキーを用いて前記配布媒体に含まれる暗号化デジタルデータを復号してデジタルデータを生成し、識別番号は、配布媒体に書き込まれているＮ個の暗号化スクランブルキーから当該復号装置に対応する１つの暗号化スクランブルキーを識別し、前記鍵管理装置は、さらに、前記配布媒体から１つの暗号化スクランブルキーを読み出す第１暗号文読出手段と、１つの復号鍵セットを読み出す復号鍵セット読出手段と、前記読み出した復号鍵セットに含まれる前記所定数の復号鍵を用いて、前記読み出した暗号化スクランブルキーを順次復号し、前記第１の所定の基準により正しく暗号化スクランブルキーを復号する復号鍵を、前記所定数の復号鍵の中から１つ選択する復号選択手段と、前記配布媒体からＮ個の暗号化スクランブルキーの読み出しが終了するまで、前記第１暗号文読出手段、前記復号鍵セット読出手段、前記復号選択手段に対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返し行うように制御し、その結果Ｎ個の復号鍵のセットが選択される第１繰返制御手段と、前記Ｍ個の暗号鍵セットから、前記選択されたＮ個の復号鍵のセットと一致する１つの暗号鍵セットを検出し、検出された暗号鍵セットにより特定される暗号装置を識別する鍵パターン検出手段とを備える。この構成によれば、鍵管理装置は、配布媒体がどの種類の暗号装置により生産されたものであるかを識別することができるという効果がある。

【００８３】ここで、前記鍵管理装置は、所定数の復号鍵からなる復号鍵セットをＮ個記憶している第１復号鍵記憶手段と、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、第１の所定の方法により１つの復号鍵を選択して１つの暗号鍵とし、Ｎ個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成手段と、前記生成された１つの暗号鍵セットを記憶する第１暗号鍵記憶手段と、Ｍ個の暗号鍵セットが生成されるまで、前記暗号鍵生成手段に対して、暗号鍵セットの生成を繰り返すように制御し、その結果、前記第１暗号鍵記憶手段はＭ個の暗号鍵セットを記憶する第２繰返制御手段と、前記第１暗号鍵記憶手段に記憶されているＭ個の暗号鍵セットをそれぞれ前記Ｍ種類の暗号装置に配布する暗号鍵セット配布手段と、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットをそれぞれ前記Ｎ種類の復号装置に配布する復号鍵セット配布手段と、Ｎ個の識別番号をそれぞれ前記Ｎ種類の復号装置に配布する識別番号配布手段と備えるように構成してもよい。この構成によれば、各復号装置には、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。

【００８４】ここで、前記第１の所定の方法とは、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、ランダムに１個の復号鍵を選択することであるように構成してもよい。この構成によれば、暗号装置に割り当てられるＮ個の暗号鍵は、各復号装置に割り当てられる所定数の復号鍵のうちの１つをランダムに選択するので、異なる暗号鍵の組合せが多くなり、異なる暗号鍵を割り当てることのできる暗号装置の数を多くすることができるという効果がある。

【００８５】ここで、前記第１の所定の方法とは、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、一様にランダムに１個の復号鍵を選択することであるように構成してもよい。この構成によれば、暗号装置に割り当てられるＮ個の暗号鍵は、各復号装置に割り当てられる所定数の復号鍵から一様にランダムに選択するので、どれか１つの種類の暗号装置が記憶する暗号鍵が暴露されたとしても、全体の暗号鍵が暴露されることがないという効果がある。

【００８６】ここで、前記Ｍ種類の暗号装置のそれぞれは、前記鍵管理装置から配布された１つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する第２暗号鍵記憶手段と、スクランブルキーを生成するスクランブルキー生成手段と、外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、前記第２暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるＮ個の暗号鍵を用いて、第２の所定の方法により、前記スクランブルキーを順次暗号化し、Ｎ個の暗号化スクランブルキーを生成する鍵暗号化手段と、前記生成された暗号化デジタルデータと前記生成されたＮ個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備えるように構成してもよい。この構成によれば、暗号装置は、各復号装置毎に、スクランブルキーを暗号化し、各復号装置は、割り当てられた復号鍵でスクランブルキーを復号するので、暗号が解読されにくいという効果がある。

【００８７】ここで、前記第２の所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【００８８】ここで、前記第２の所定の方法とは、前記スクランブルキーを暗号化してＮ個の暗号化スクランブ

ルキーを生成し、さらに、固定値からなる固定情報を暗号化してＮ個の暗号化固定情報を生成することであり、前記媒体書込手段は、暗号化デジタルデータとＮ個の暗号化スクランブルキーとＮ個の暗号化固定情報とを配布媒体に書き込むように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【００８９】ここで、前記復号選択手段は、前記復号鍵セットから復号鍵を順次読み出す第１復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第１復号文生成手段と、前記第１の所定の基準により、復号文が正しく復号されているかどうかを検査する第１復号文検査手段と、前記復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第１復号鍵読出手段、前記第１復号文生成手段、前記第１復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第３繰返制御手段と、前記復号文検査手段により正しく復号されたと検査された際に用いられた復号鍵を出力する鍵出力手段とを備えるように構成してもよい。この構成によれば、鍵管理装置は、配布媒体がどの種類の暗号装置により生産されたものであるかを識別することができるという効果がある。

【００９０】ここで、前記第１の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【００９１】ここで、前記配布媒体は、さらに、前記暗号鍵セットに含まれるＮ個の暗号鍵を用いて固定値からなる固定情報が暗号化されたＮ個の暗号化固定情報を含み、前記鍵管理装置は、さらに、Ｎ個の暗号化固定情報を読み出す暗号化固定情報読出手段と、前記Ｎ個の復号鍵セットを用いて、前記読み出したＮ個の暗号化固定情報をそれぞれ復号する暗号化固定情報復号手段とを含み、前記第１の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して

暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【００９２】ここで、前記Ｎ種類の復号装置のそれぞれは、前記鍵管理装置から識別番号を受信し、受信した識別番号を記憶する識別番号記憶手段と、前記鍵管理装置から配布された１つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する第２復号鍵記憶手段と、前記配布媒体から前記受信した識別番号により識別される１つの暗号化スクランブルキーを読み出す第２暗号文読出手段と、前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、前記第２復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す第２復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第２復号文生成手段と、前記第１の所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文をスクランブルキーとする第２復号文検査手段と、復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第２復号鍵読出手段、前記第２復号文生成手段、前記第２復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第４繰返制御手段と、前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えるように構成してもよい。この構成によれば、鍵管理装置は、復号装置に対して、暗号装置が作成したＮ個の暗号文のうち、その復号装置に対応する暗号文を識別する情報を予め通知し、復号装置はこの情報を用いて暗号文を識別することができるという効果がある。

【００９３】ここで、前記第１の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【００９４】ここで、前記配布媒体は、さらに、前記暗号鍵セットに含まれるＮ個の暗号鍵を用いて固定値からなる固定情報が暗号化されたＮ個の暗号化固定情報を含み、前記復号装置は、さらに、前記識別番号により識別される１つの暗号化固定情報を読み出す暗号化固定情報読出手段と、前記復号鍵セットに含まれる所定数の復号

鍵を用いて、前記読み出した暗号化固定情報を復号する暗号化固定情報復号手段とを備え、前記第１の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【００９５】ここで、前記Ｍ種類の暗号装置のそれぞれは、前記鍵管理装置から配布された１つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する第２暗号鍵記憶手段と、スクランブルキーを生成するスクランブルキー生成手段と、外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、前記第２暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるＮ個の暗号鍵を用いて、第２の所定の方法により、前記スクランブルキーを順次暗号化し、Ｎ個の暗号化スクランブルキーを生成する鍵暗号化手段と、前記生成された暗号化デジタルデータと前記生成されたＮ個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備え、前記鍵管理装置において、前記復号選択手段は、前記復号鍵セットから復号鍵を順次読み出す第１復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第１復号文生成手段と、前記第１の所定の基準により、復号文が正しく復号されているかどうかを検査する第１復号文検査手段と、前記復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第１復号鍵読出手段、前記第１復号文生成手段、前記第１復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第３繰返制御手段と、前記復号文検査手段により正しく復号されたと検査された際に用いられた復号鍵を出力する鍵出力手段とを備えるように構成してもよい。この構成によれば、暗号装置は、各復号装置毎にスクランブルキーを暗号化し、鍵管理装置は、配布媒体がどの種類の暗号装置により生産されたものであるかを識別することができるという効果がある。

【００９６】ここで、前記第１の所定の基準とは、前記復号文に固定情報が含まれることであり、前記第２の所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【００９７】ここで、前記第２の所定の方法とは、前記スクランブルキーを暗号化してＮ個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化してＮ個の暗号化固定情報を生成することであり、前記媒体書込手段は、暗号化デジタルデータとＮ個の暗号化スクランブルキーとＮ個の暗号化固定情報とを配布媒体に書き込み、前記鍵管理装置は、Ｎ個の暗号化固定情報を読み出す暗号化固定情報読出手段と、Ｎ個の復号鍵セットを用いて、前記読み出したＮ個の暗号化固定情報をそれぞれ復号する暗号化固定情報復号手段とを備え、前記第１の所定の基準とは、Ｎ個の暗号化固定情報を復号し、さらに、固定情報を生成することであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【００９８】ここで、前記Ｍ種類の暗号装置のそれぞれは、前記鍵管理装置から配布された１つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する第２暗号鍵記憶手段と、スクランブルキーを生成するスクランブルキー生成手段と、外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、前記第２暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるＮ個の暗号鍵を用いて、第２の所定の方法により、前記スクランブルキーを順次暗号化し、Ｎ個の暗号化スクランブルキーを生成する鍵暗号化手段と、前記生成された暗号化デジタルデータと前記生成されたＮ個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備え、前記Ｎ種類の復号装置のそれぞれは、前記鍵管理装置から識別番号を受信し、受信した識別番号を記憶する識別番号記憶手段と、前記鍵管理装置から配布された１つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する第２復号鍵記憶手段と、前記配布媒体から前記受信した識別番号により識別される１つの暗号化スクランブルキーを読み出す第２暗号文読出手段と、前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、前記第２復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す第２復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出

した暗号化スクランブルキーを復号し、復号文を生成する第２復号文生成手段と、前記第１の所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文はスクランブルキーを含む第２復号文検査手段と、復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第２復号鍵読出手段、前記第２復号文生成手段、前記第２復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第４繰返制御手段と、前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えるように構成してもよい。この構成によれば、各復号装置には、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。

【００９９】ここで、前記第１の所定の基準とは、前記復号文に固定情報が含まれることであり、前記第２の所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【０１００】ここで、前記第２の所定の方法とは、前記スクランブルキーを暗号化してＮ個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化してＮ個の暗号化固定情報を生成することであり、前記媒体書込手段は、暗号化デジタルデータとＮ個の暗号化スクランブルキーとＮ個の暗号化固定情報とを配布媒体に書き込み、前記復号装置は、さらに、前記識別番号により識別される暗号化固定情報を読み出す暗号化固定情報読出手段と、復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を読み出す暗号化固定情報復号手段とを備え、前記第１の所定の基準とは、暗号化固定情報を復号し、さらに、固定情報を生成することであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【０１０１】ここで、前記鍵管理装置は、所定数の復号鍵からなる復号鍵セットをＮ個記憶している第１復号鍵記憶手段と、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、第１の所定の方法により１つの復号鍵を選択して１つの暗号鍵とし、Ｎ個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成手段と、前記生成された１つの暗号鍵セットを記憶する第１暗号鍵記憶手段と、Ｍ個の暗号鍵セットが生成されるまで、前記暗号鍵生成手段に対して、暗号鍵セットの生成を繰り返すように制御し、この結果、前記第１暗号鍵記憶手段はＭ個の暗号鍵セットを記憶する第２繰返制御手段と、前記第１暗号鍵記憶手段に記憶されているＭ個の暗号鍵セットをそれぞれ前記Ｍ種類の暗号装置に配布する暗号鍵セット配布手段と、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットをそれぞれ前記Ｎ種類の復号装置に配布する復号鍵セット配布手段と、識別番号を前記Ｎ種類の復号装置に配布する識別番号配布手段とを備え、前記Ｎ種類の復号装置のそれぞれは、前記鍵管理装置から識別番号を受信し、受信した識別番号を記憶する識別番号記憶手段と、前記鍵管理装置から配布された１つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する第２復号鍵記憶手段と、前記配布媒体から前記受信した識別番号により識別される１つの暗号化スクランブルキーを読み出す第２暗号文読出手段と、前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、前記第２復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す第２復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第２復号文生成手段と、前記第１の所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文をスクランブルキーとする第２復号文検査手段と、復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第２復号鍵読出手段、前記第２復号文生成手段、前記第２復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第４繰返制御手段と、前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えるように構成してもよい。この構成によれば、各復号装置には、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。また、鍵管理装置は、復号装置に対して、

暗号装置が作成したＮ個の暗号文のうち、その復号装置に対応する暗号文を識別する情報を予め通知し、復号装置はこの情報を用いて暗号文を識別することができるという効果がある。

【０１０２】ここで、前記第１の所定の方法とは、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、ランダムに１個の復号鍵を選択することであるように構成してもよい。この構成によれば、暗号装置に割り当てられるＮ個の暗号鍵は、各復号装置に割り当てられる所定数の復号鍵のうちの１つをランダムに選択するので、異なる暗号鍵の組合せが多くなり、異なる暗号鍵を割り当てることのできる暗号装置の数を多くすることができるという効果がある。

【０１０３】ここで、前記第１の所定の方法とは、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、一様にランダムに１個の復号鍵を選択することであるように構成してもよい。この構成によれば、暗号装置に割り当てられるＮ個の暗号鍵は、各復号装置に割り当てられる所定数の復号鍵から一様にランダムに選択するので、どれか１つの種類の暗号装置が記憶する暗号鍵が暴露されたとしても、全体の暗号鍵が暴露されることがないという効果がある。

【０１０４】ここで、前記第１の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【０１０５】ここで、前記配布媒体は、さらに、前記暗号鍵セットに含まれるＮ個の暗号鍵を用いて固定値からなる固定情報が暗号化されたＮ個の暗号化固定情報を含み、前記復号装置は、さらに、前記識別番号により識別される１つの暗号化固定情報を読み出す暗号化固定情報読出手段と、前記復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を復号する暗号化固定情報復号手段とを備え、前記第１の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【０１０６】また、本発明は、Ｍ（Ｍは２以上の整数）種類の暗号装置とＮ（Ｎは２以上の整数）種類の復号装置に鍵情報を配布する鍵管理装置であって、所定数の復号鍵からなる復号鍵セットをＮ個記憶している復号鍵記憶手段と、前記復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、第１の所定の方法により１つの復号鍵を選択して１つの暗号鍵とし、Ｎ個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成手段と、前記生成された１つの暗号鍵セットを記憶する暗号鍵記憶手段と、Ｍ個の暗号鍵セットが生成されるまで、前記暗号鍵生成手段に対して、暗号鍵セットの生成を繰り返すように制御し、その結果、前記暗号鍵記憶手段はＭ個の暗号鍵セットを記憶する繰返制御手段と、前記第１暗号鍵記憶手段に記憶されているＭ個の暗号鍵セットをそれぞれＭ種類の暗号装置に配布する暗号鍵セット配布手段と、前記第１復号鍵記憶手段に記憶されているＮ個の復号鍵セットをそれぞれＮ種類の復号装置に配布する復号鍵セット配布手段と、Ｎ個の識別番号をそれぞれＮ種類の復号装置に配布する識別番号配布手段とを備える。この構成によれば、各復号装置には、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。

【０１０７】また、本発明は、鍵管理装置から配布される鍵情報を用いて、デジタルデータを暗号化して配布媒体に書き込む暗号装置であって、鍵管理装置から配布された１つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する暗号鍵記憶手段と、スクランブルキーを生成するスクランブルキー生成手段と、外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、前記暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるＮ（Ｎは２以上の整数）個の暗号鍵を用いて、所定の方法により、前記スクランブルキーを順次暗号化し、Ｎ個の暗号化スクランブルキーを生成する鍵暗号化手段と、前記生成された暗号化デジタルデータと前記生成されたＮ個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備える。この構成によれば、暗号装置は、各復号装置毎に、スクランブルキーを暗号化し、各復号装置は、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。

【０１０８】また、本発明は、鍵管理装置から配布された鍵情報を用いて、配布媒体に書かれた暗号化デジタルデータを復号する復号装置であって、配布媒体に書き込

まれているＮ個の暗号化スクランブルキーから当該復号装置に対応する１つの暗号化スクランブルキーを識別する識別番号を鍵管理装置から受信し、受信した識別番号を記憶する識別番号記憶手段と、鍵管理装置から配布された１つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する復号鍵記憶手段と、前記配布媒体から前記受信した識別番号により識別される１つの暗号化スクランブルキーを読み出す暗号文読出手段と、前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、前記復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する復号文生成手段と、所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文はスクランブルキーを含む復号文検査手段と、復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記復号鍵読出手段、前記復号文生成手段、前記復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する繰返制御手段と、前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備える。この構成によれば、各復号装置には、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。

【０１０９】また、本発明は、配布媒体にデジタルデータを暗号化して書き込んだ暗号装置の種類を識別する鍵管理装置であって、前記配布媒体から１つの暗号化スクランブルキーを読み出す暗号文読出手段と、１つの復号鍵セットを読み出す復号鍵セット読出手段と、前記読み出した復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化スクランブルキーを順次復号し、所定の基準により正しく暗号化スクランブルキーを復号する復号鍵を、前記所定数の復号鍵の中から１つ選択する復号選択手段と、前記配布媒体からＮ個の暗号化スクランブルキーの読み出しが終了するまで、前記暗号文読出手段、前記復号鍵セット読出手段、前記復号選択手段に対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返し行うように制御し、この結果、Ｎ個の復号鍵のセットが選択される繰返制御手段と、前記Ｍ個の暗号鍵セットから、前記選択されたＮ個の復号鍵のセットと一致する１つの暗号鍵セットを検出し、検出された暗号鍵セットにより特定される暗号装置を識別する鍵パターン検出手段とを備える。この構成によれば、鍵管理装置は、配布媒体がどの種類の暗号装置により生産されたものであるかを識別することができるという効果がある。

【０１１０】また、本発明は、Ｍ（Ｍは２以上の整数）種類の暗号装置とＮ（Ｎは２以上の整数）種類の復号装置に鍵情報を配布し、所定数の復号鍵からなる復号鍵セットをＮ個記憶している復号鍵記憶手段を備える鍵管理装置において用いられる鍵管理方法であって、前記復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、所定の方法により１つの復号鍵を選択して１つの暗号鍵とし、Ｎ個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成ステップと、Ｍ個の暗号鍵セットが生成されるまで、前記暗号鍵生成ステップに対して、暗号鍵セットの生成を繰り返すように制御し、この結果、Ｍ個の暗号鍵セットが生成される繰返制御ステップと、暗号鍵生成ステップにより生成されたＭ個の暗号鍵セットをそれぞれＭ種類の暗号装置に配布する暗号鍵セット配布ステップと、前記復号鍵記憶手段に記憶されているＮ個の復号鍵セットをそれぞれＮ種類の復号装置に配布する復号鍵セット配布ステップと、Ｎ個の識別番号をそれぞれＮ種類の復号装置に配布する識別番号配布ステップとを含む。この方法を用いると、各復号装置には、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。

【０１１１】ここで、前記所定の方法とは、前記復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、ランダムに１個の復号鍵を選択することであるように構成してもよい。この方法を用いると、暗号装置に割り当てられるＮ個の暗号鍵は、各復号装置に割り当てられる所定数の復号鍵のうちの１つをランダムに選択するので、異なる暗号鍵の組合せが多くなり、異なる暗号鍵を割り当てることのできる暗号装置の数を多くすることができるという効果がある。

【０１１２】ここで、前記所定の方法とは、前記復号鍵記憶手段に記憶されているＮ個の復号鍵セットのそれぞれから、一様にランダムに１個の復号鍵を選択することであるように構成してもよい。この方法を用いると、暗号装置に割り当てられるＮ個の暗号鍵は、各復号装置に割り当てられる所定数の復号鍵から一様にランダムに選択するので、どれか１つの種類の暗号装置が記憶する暗号鍵が暴露されたとしても、全体の暗号鍵が暴露されることがないどいう効果がある。

【０１１３】また、本発明は、鍵管理装置から配布される鍵情報を用いて、デジタルデータを暗号化して配布媒体に書き込み、鍵管理装置から配布された１つの暗号鍵セットを受信し受信した前記暗号鍵セットを記憶する暗号鍵記憶手段を備える暗号装置において用いられる暗号

方法であって、スクランブルキーを生成するスクランブルキー生成ステップと、外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化ステップと、前記暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるＮ（Ｎは２以上の整数）個の暗号鍵を用いて、所定の方法により、前記スクランブルキーを順次暗号化し、Ｎ個の暗号化スクランブルキーを生成する鍵暗号化ステップと、前記生成された暗号化デジタルデータと前記生成されたＮ個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込ステップとを含む。この方法を用いると、暗号装置は、各復号装置毎にスクランブルキーを暗号化し、各復号装置は、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。

【０１１４】ここで、前記所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであるように構成してもよい。この方法を用いると、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【０１１５】ここで、前記所定の方法とは、前記スクランブルキーを暗号化してＮ個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化してＮ個の暗号化固定情報を生成することであり、前記媒体書込ステップは、暗号化デジタルデータとＮ個の暗号化スクランブルキーとＮ個の暗号化固定情報とを配布媒体に書き込むように構成してもよい。この方法を用いると、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【０１１６】また、本発明は、鍵管理装置から配布された鍵情報を用いて、配布媒体に書かれた暗号化デジタルデータを復号し、鍵管理装置から識別番号を受信し受信した識別番号を記憶する識別番号記憶手段と、鍵管理装置から配布された１つの復号鍵セットを受信し受信した前記復号鍵セットを記憶する復号鍵記憶手段とを備える復号装置において用いられる復号方法であって、前記識別番号は配布媒体に書き込まれているＮ個の暗号化スクランブルキーから当該復号装置に対応する１つの暗号化スクランブルキーを識別し、前記配布媒体から前記受信した識別番号により識別される１つの暗号化スクランブルキーを読み出す暗号文読出ステップと、前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出ステップと、前記復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す復号鍵読出ステップと、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する復号文生成ステップと、所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文はスクランブルキーを含む復号文検査ステップと、復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記復号鍵読出ステップ、前記復号文生成ステップ、前記復号文検査ステップに対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する繰返制御ステップと、前記復号文検査ステップにより正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号ステップとを含む。この方法を用いると、各復号装置には、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。

【０１１７】ここで、前記所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この方法を用いると、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【０１１８】ここで、前記配布媒体は、さらに、暗号鍵セットに含まれるＮ個の暗号鍵を用いて固定値からなる固定情報が暗号化されたＮ個の暗号化固定情報を含み、前記復号方法は、さらに、前記識別番号により識別される１つの暗号化固定情報を読み出す暗号化固定情報読出ステップと、復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を復号する暗号化固定情報復号ステップとを含み、前記所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この方法を用いると、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復

号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【０１１９】また、本発明は、配布媒体にデジタルデータを暗号化して書き込んだ暗号装置の種類を識別する鍵管理装置において用いられる鍵管理方法であって、前記配布媒体から１つの暗号化スクランブルキーを読み出す暗号文読出ステップと、１つの復号鍵セットを読み出す復号鍵セット読出ステップと、前記読み出した復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化スクランブルキーを順次復号し、所定の基準により正しく暗号化スクランブルキーを復号する復号鍵を、前記所定数の復号鍵の中から１つ選択する復号選択ステップと、前記配布媒体からＮ（Ｎは２以上の整数）個の暗号化スクランブルキーの読み出しが終了するまで、前記暗号文読出ステップ、前記復号鍵セット読出ステップ、前記復号選択ステップに対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返し行うように制御し、この結果、Ｎ個の復号鍵のセットが選択される繰返制御ステップと、前記Ｍ個の暗号鍵セットから、前記選択されたＮ個の復号鍵のセットと一致する１つの暗号鍵セットを検出し、検出された暗号鍵セットにより特定される暗号装置の種類を識別する鍵パターン検出ステップとを含む。この方法を用いると、鍵管理装置は、配布媒体がどの種類の暗号装置により生産されたものであるかを識別することができるという効果がある。

【０１２０】ここで、前記所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この方法を用いると、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【０１２１】ここで、前記配布媒体は、さらに、暗号鍵セットに含まれるＮ個の暗号鍵を用いて固定値からなる固定情報が暗号化されたＮ個の暗号化固定情報を含み、前記鍵管理方法は、さらに、Ｎ個の暗号化固定情報を読み出す暗号化固定情報読出ステップと、Ｎ個の復号鍵セットを用いて、前記読み出したＮ個の暗号化固定情報を復号する暗号化固定情報復号ステップとを含み、前記所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この方法を用いると、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【０１２２】

【図面の簡単な説明】

【図１】図１は、本発明に係る１つの実施の形態としての暗号システム１０の構成を示すブロック図である。

【図２】図２は、図１に示す暗号システム１０の鍵管理装置１００の構成を示すブロック図である。

【図３】図３は、図２に示す鍵管理装置１００の復号選択部１３４の構成を示すブロック図である。

【図４】図４は、図２に示す鍵管理装置１００の暗号鍵テーブル１１４と復号鍵テーブル１１２の構成を示す。

【図５】図５は、図２に示す鍵管理装置１００の復号鍵テーブル１１２の一例を示す。

【図６】図６は、図２に示す鍵管理装置１００の暗号鍵テーブル１１４の一例を示す。

【図７】図７は、図３に示す復号選択部１３４の復号文生成部１４３により復号されるスクランブルキーを含む復号文の構成を示す。

【図８】図８は、図１に示す暗号システム１０の鍵管理装置１００の鍵生成と鍵の配布の動作を示すフローチャートである。

【図９】図９は、図１に示す暗号システム１０の鍵管理装置１００の暗号装置の種類を特定する動作を示すフローチャートである。

【図１０】図１０は、図１に示す暗号システム１０の暗号装置２００の構成を示すブロック図である。

【図１１】図１１は、図１０に示す暗号装置２００の鍵暗号化部２０４の構成を示すブロック図である。

【図１２】図１２は、図１０に示す暗号装置２００のデジタルデータ暗号化部２０２の動作を示すフローチャートである。

【図１３】図１３は、図１０に示す暗号装置２００の動作を示すフローチャートである。

【図１４】図１４は、配布媒体の構成を示す。

【図１５】図１５は、図１に示す暗号システム１０の復号装置３００の構成を示すブロック図である。

【図１６】図１６は、図１５に示す復号装置３００の復号文生成部３０６の構成を示すブロック図である。

【図１７】図１７は、図１５に示す復号装置３００のデジタルデータ復号部３０９の動作を示すフローチャートである。

【図１８】図１８は、図１５に示す復号装置３００の動作を示すフローチャートである。

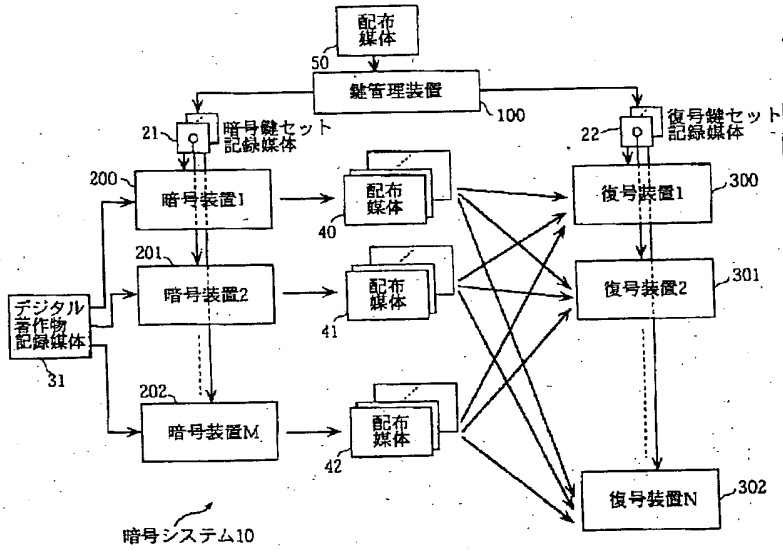
【符号の説明】

１０　　暗号システム

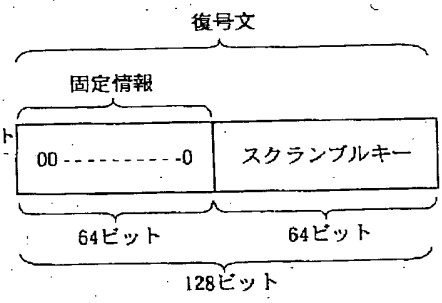
２１	暗号鍵セット記録媒体
２２	復号鍵セット記録媒体
３１	デジタル著作物記録媒体
４０～４２、５０	配布媒体
１００	鍵管理装置
１１１	暗号鍵セット配布部
１１２	復号鍵テーブル
１１３	暗号鍵生成部
１１４	暗号鍵テーブル
１１５	暗号鍵生成制御部
１１６	暗号鍵セット配布部
１２１	識別番号配布部
１２２	識別番号記憶部
１３１	復号選択制御部
１３２	復号鍵セット読出部
１３３	暗号文読出部
１３４	復号選択部
１３５	鍵パターン検出部
１３６	暗号装置管理処理部
１４１	復号鍵読出部
１４２	復号制御部
１４３	復号文生成部
１４４	復号文検査部

１４５	鍵出力部
２００～２０２	暗号装置
２０３	スクランブルキー生成部
２０４	鍵暗号化部
２０５	暗号鍵記憶部
２０６	デジタルデータ暗号化部
２１１、２１４	分解部
２１２、２１３	ＤＥＳ暗号化部
２１５	結合部
３００～３０２	復号装置
３０３	復号鍵読出部
３０４	復号検査制御部
３０５	暗号文読出部
３０６	復号文生成部
３０７	復号文検査部
３０８	デジタルデータ読出部
３０９	デジタルデータ復号部
３１０	表示部
３１１	識別番号記憶部
３１２	復号鍵記憶部
３２１、３２４	分解部
３２２、３２３	ＤＥＳ復号部
３２５	結合部

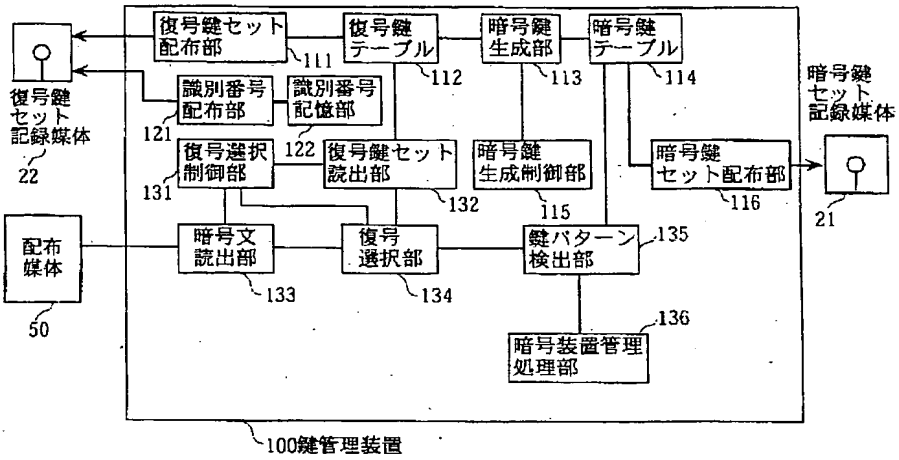
【図１】



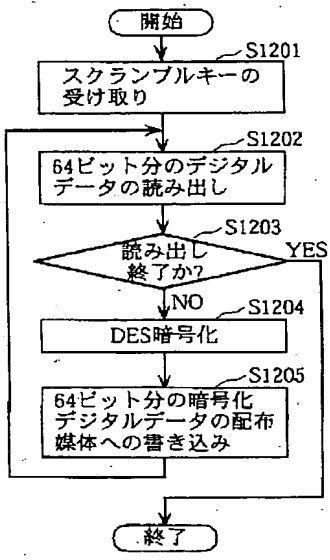
【図７】



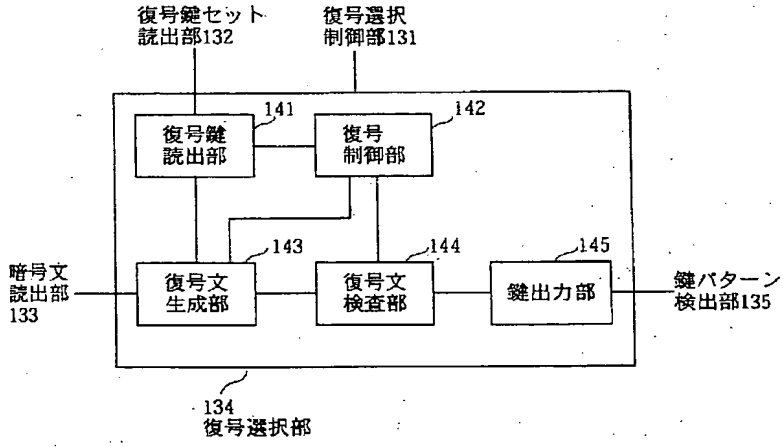
【図２】



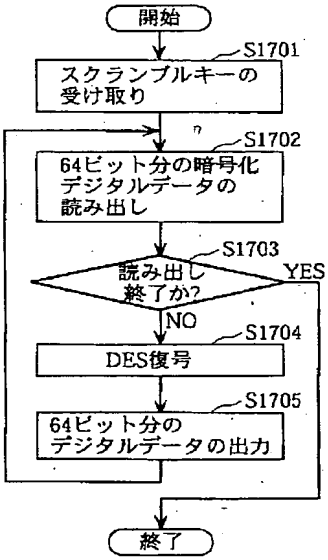
【図１２】



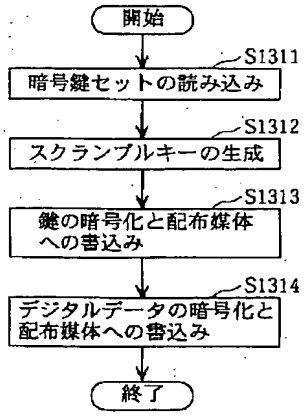
【図３】



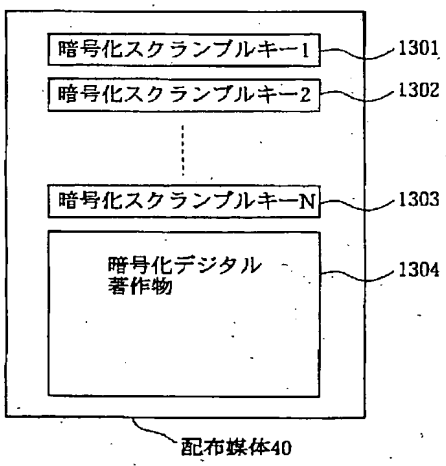
【図１７】



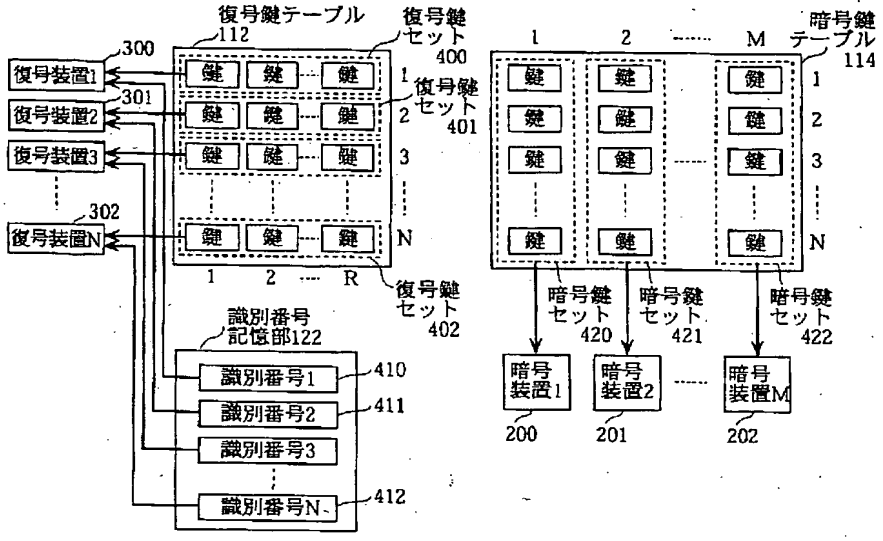
【図１３】



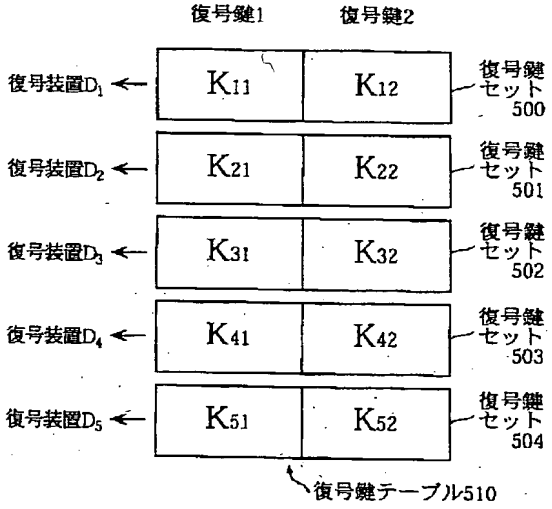
【図１４】



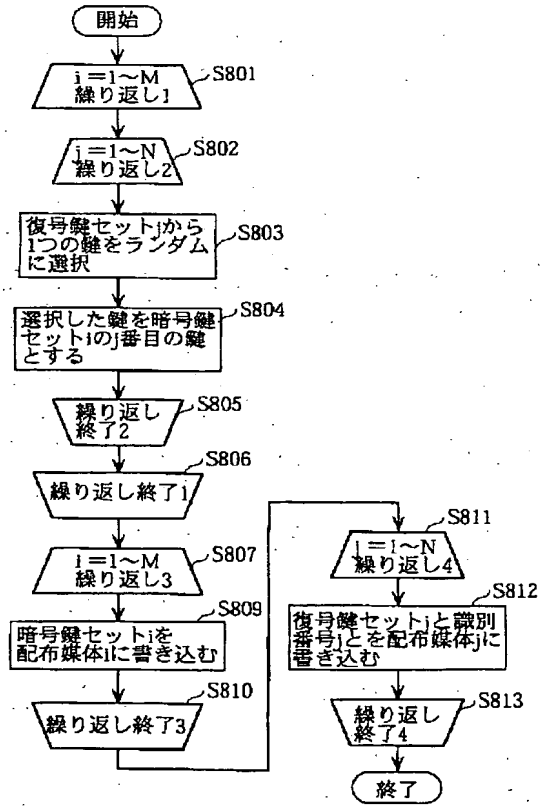
【図４】


復号鍵テーブル
112
復号鍵セット
400
復号鍵セット
401
復号鍵セット
402
復号装置1
復号装置2
復号装置3
復号装置N
300
301
302
鍵
識別番号記憶部122
識別番号1
識別番号2
識別番号3
識別番号N
410
411
412
暗号鍵テーブル
114
暗号鍵セット
420
暗号鍵セット
421
暗号鍵セット
422
暗号装置1
暗号装置2
暗号装置M
200
201
202

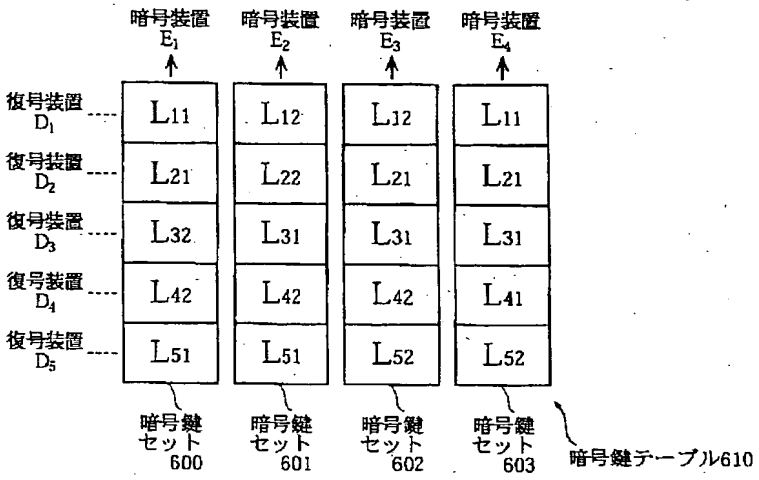
【図５】


復号鍵1
復号鍵2
復号装置D1
復号装置D2
復号装置D3
復号装置D4
復号装置D5
K11
K12
K21
K22
K31
K32
K41
K42
K51
K52
復号鍵セット
500
復号鍵セット
501
復号鍵セット
502
復号鍵セット
503
復号鍵セット
504
復号鍵テーブル510

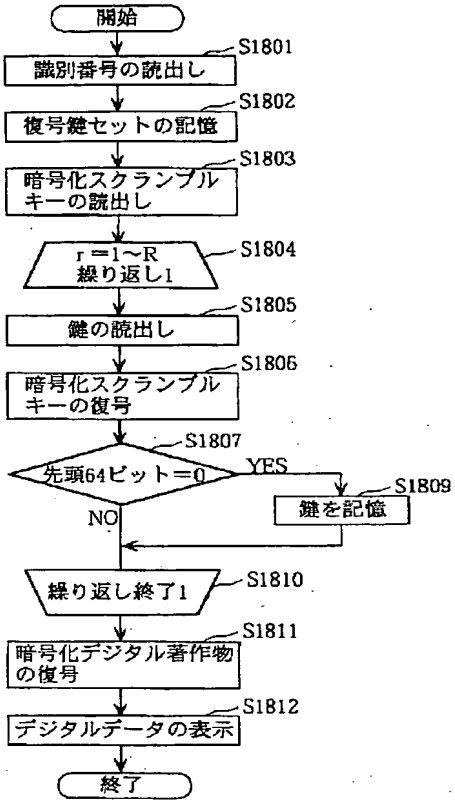
【図８】


開始
i＝1～M
繰り返し1
S801
j＝1～N
繰り返し2
S802
復号鍵セットjから1つの鍵をランダムに選択
S803
選択した鍵を暗号鍵セットiのj番目の鍵とする
S804
繰り返し終了2
S805
繰り返し終了1
S806
i＝1～M
繰り返し3
S807
暗号鍵セットiを配布媒体iに書き込む
S809
繰り返し終了3
S810
j＝1～N
繰り返し4
S811
復号鍵セットjと識別番号jとを配布媒体jに書き込む
S812
繰り返し終了4
S813
終了

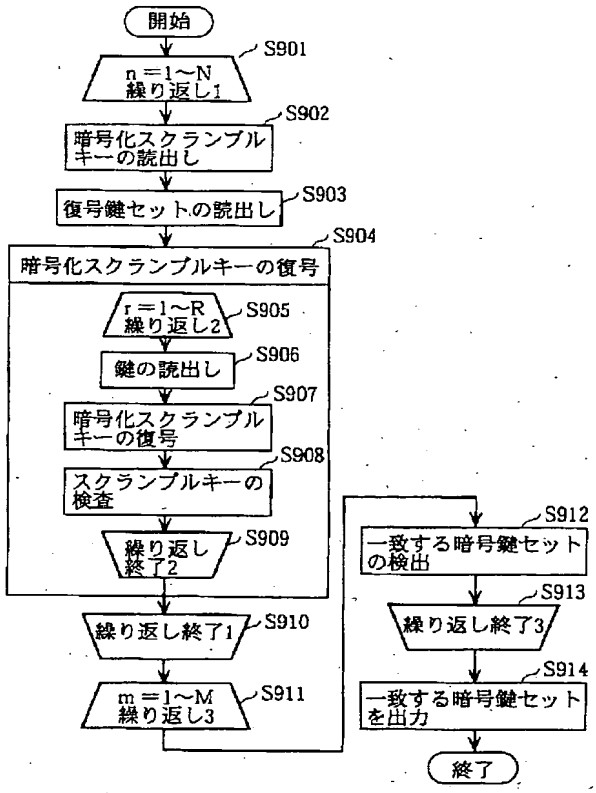
【図６】


暗号装置 E1
暗号装置 E2
暗号装置 E3
暗号装置 E4
復号装置 D1
復号装置 D2
復号装置 D3
復号装置 D4
復号装置 D5
L11 L12 L12 L11
L21 L22 L21 L21
L32 L31 L31 L31
L42 L42 L42 L41
L51 L51 L52 L52
暗号鍵セット 600
暗号鍵セット 601
暗号鍵セット 602
暗号鍵セット 603
暗号鍵テーブル610

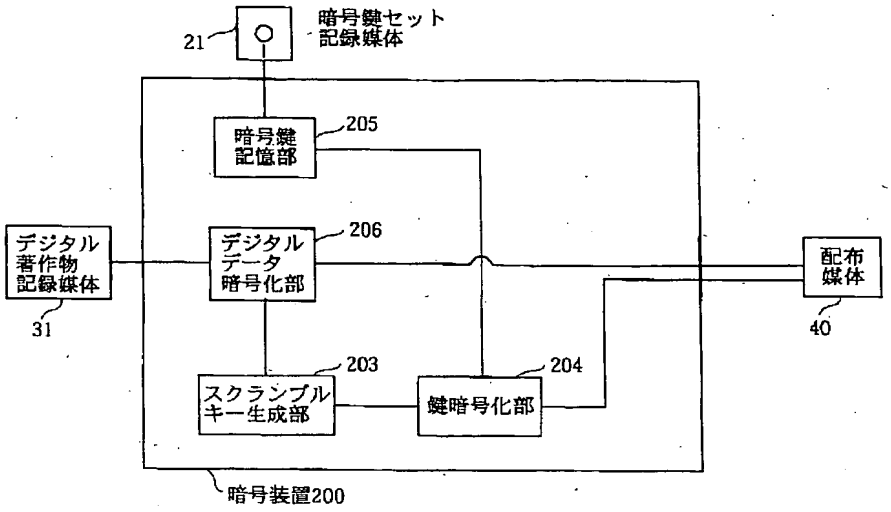
【図１８】


開始
S1801
識別番号の読出し
S1802
復号鍵セットの記憶
S1803
暗号化スクランブルキーの読出し
S1804
r＝1～R 繰り返し1
S1805
鍵の読出し
S1806
暗号化スクランブルキーの復号
S1807
先頭64ビット＝0
YES
S1809
鍵を記憶
NO
S1810
繰り返し終了1
S1811
暗号化デジタル著作物の復号
S1812
デジタルデータの表示
終了

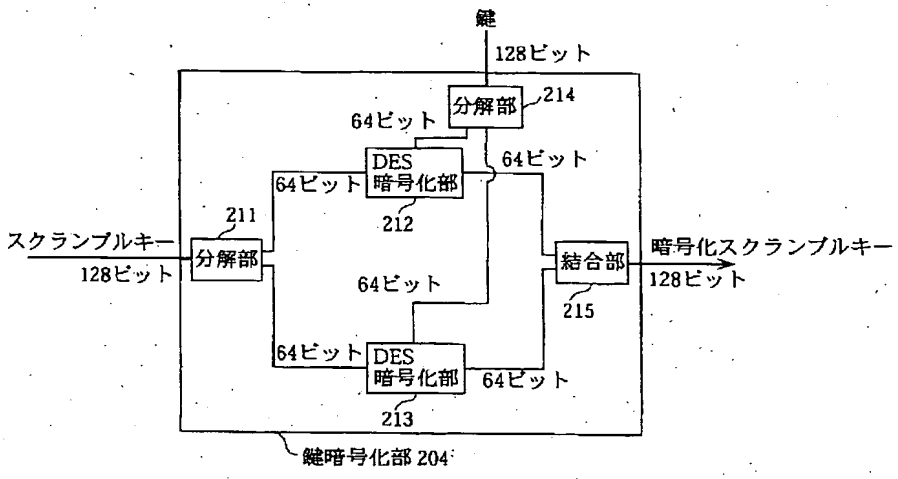
【図９】


開始
S901
n＝1～N 繰り返し1
S902
暗号化スクランブルキーの読出し
S903
復号鍵セットの読出し
S904
暗号化スクランブルキーの復号
S905
r＝1～R 繰り返し2
S906
鍵の読出し
S907
暗号化スクランブルキーの復号
S908
スクランブルキーの検査
S909
繰り返し終了2
S910
繰り返し終了1
S911
m＝1～M 繰り返し3
S912
一致する暗号鍵セットの検出
S913
繰り返し終了3
S914
一致する暗号鍵セットを出力
終了

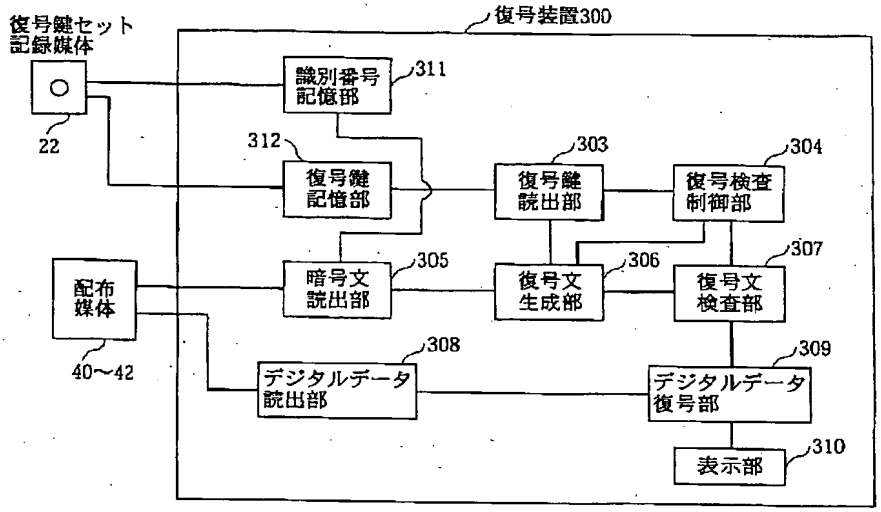
【図１０】


暗号鍵セット
記録媒体
21
暗号鍵
記憶部
205
デジタル
著作物
記録媒体
31
デジタル
データ
暗号化部
206
配布
媒体
40
203
スクランブル
キー生成部
204
鍵暗号化部
暗号装置200

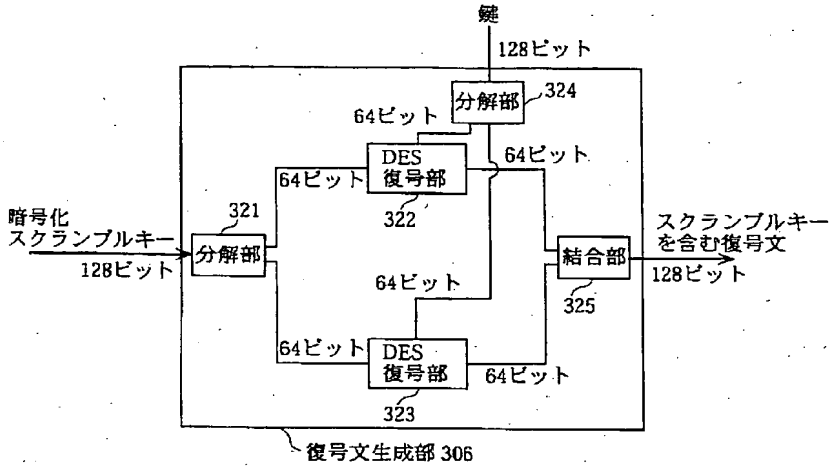
【図１１】


鍵
128ビット
分解部
214
64ビット
DES
暗号化部
64ビット
64ビット
212
211
スクランブルキー
128ビット
分解部
64ビット
結合部
暗号化スクランブルキー
128ビット
215
64ビット
DES
暗号化部
64ビット
213
鍵暗号化部 204

【図１５】


復号鍵セット
記録媒体
22
復号装置300
識別番号
記憶部
311
312
復号鍵
記憶部
303
復号鍵
読出部
304
復号検査
制御部
配布
媒体
40～42
暗号文
読出部
305
復号文
生成部
306
307
復号文
検査部
308
デジタルデータ
読出部
309
デジタルデータ
復号部
表示部
310

【図１６】


鍵
128ビット
分解部
324
64ビット
DES
復号部
64ビット
64ビット
322
暗号化
スクランブルキー
128ビット
321
分解部
結合部
スクランブルキー
を含む復号文
128ビット
64ビット
325
64ビット
DES
復号部
64ビット
323
復号文生成部 306